WAP3205

Wireless N Access Point

User's Guide

Default Login Details

IP Address	http://192.168.1.2
Password	1234

Version 1.00
Edition 3, 04/2012

ZyXEL

www.zyxel.com

Copyright © 2012
ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

Contents Overview

User's Guide 9

Getting to Know Your WAP3205 11
WAP3205 Modes 15
Access Point Mode 17
Client Mode 23
Universal Repeater Mode 35
Introducing the Web Configurator 43
Connection Wizard 49
Tutorials 59

Technical Reference 79

Monitor 81
Wireless LAN 85
LAN 101
Maintenance 105
Troubleshooting 115

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **9**

Chapter 1
Getting to Know Your WAP3205 ..... **11**

1.1 Overview 11
1.2 Applications 11
1.3 Ways to Manage the WAP3205 11
1.4 Good Habits for Managing the WAP3205 12
1.5 LEDs 12
1.6 Wall Mounting 13

Chapter 2
WAP3205 Modes **15**

2.1 Overview 15
2.1.1 Device Modes 15

Chapter 3
Access Point Mode **17**

3.1 Overview 17
3.2 What You Can Do 17
3.3 What You Need to Know 17
3.3.1 Setting your WAP3205 to AP Mode 17
3.3.2 Configuring your WLAN, LAN and Maintenance Settings 18
3.4 AP Mode Status Screen 18

Chapter 4
Client Mode **23**

4.1 Overview 23
4.2 What You Can Do 23
4.3 What You Need to Know 23
4.4 Setting your WAP3205 to Client Mode 24
4.5 Client Mode Status Screen 24
4.6 Wireless LAN Profile Screen 26
4.6.1 Adding a New WLAN Profile 27

4.7 Site Survey Screen 31
4.8 WPS Screen 32

Chapter 5
Universal Repeater Mode 35

5.1 Overview 35
5.2 What You Can Do 35
5.3 What You Need to Know 36
5.4 Setting your WAP3205 to Universal Repeater Mode 36
5.5 Universal Repeater Mode Status Screen 36
5.6 Universal Repeater Screen 39
5.6.1 No Security 39
5.6.2 Static WEP 40
5.6.3 WPA(2)-PSK 41

Chapter 6
Introducing the Web Configurator 43

6.1 Overview 43
6.2 Accessing the Web Configurator 43
6.2.1 Login Screen 43
6.2.2 Password Screen 44
6.2.3 Home Screen 45
6.3 Resetting the WAP3205 47
6.3.1 Procedure to Use the Reset Button 47

Chapter 7
Connection Wizard 49

7.1 Overview 49
7.2 Accessing the Wizard 49
7.2.1 Device Password 49
7.2.2 Operation Mode 50
7.2.3 Wireless Configuration 50

Chapter 8
Tutorials 59

8.1 Overview 59
8.2 Connecting to the Internet from an Access Point 59
8.3 Configuring Wireless Security Using WPS 59
8.3.1 Push Button Configuration (PBC) 60
8.3.2 PIN Configuration 61
8.4 Enabling and Configuring Wireless Security (No WPS) 62
8.4.1 Configure Your Notebook 64
8.5 Using Multiple SSIDs on the WAP3205 66

8.5.1 Configuring Security Settings of Multiple SSIDs 67
8.6 Connecting the WAP3205 (in Universal Repeater Mode) to an AP or Wireless Router 70
8.7 Connecting the WAP3205 (in Client Mode) to an AP or Wireless Router 74
8.7.1 Connecting to a Wireless Network Using Site Survey 74
8.7.2 Connecting to a Wireless Network Using a Profile 76
8.7.3 Deploying the WAP3205 in your Network 77

Part II: Technical Reference 79

Chapter 9
Monitor 81

9.1 Overview 81
9.2 What You Can Do 81
9.3 Log 81
9.4 Packet Statistics 82
9.5 WLAN Station Status 83

Chapter 10
Wireless LAN 85

10.1 Overview 85
10.2 What You Can Do 85
10.3 What You Should Know 86
10.3.1 Wireless Security Overview 86
10.4 General Wireless LAN Screen 88
10.5 Wireless Security Screen 89
10.5.1 No Security 89
10.5.2 WEP Encryption 90
10.5.3 WPA-PSK/WPA2-PSK 92
10.6 MAC Filter 93
10.7 Wireless LAN Advanced Screen 94
10.8 Quality of Service (QoS) Screen 95
10.9 WPS Screen 96
10.10 WPS Station Screen 97
10.11 Scheduling Screen 97
10.12 WDS Screen 98

Chapter 11
LAN 101

11.1 Overview 101
11.2 What You Can Do 101
11.3 What You Need To Know 101

11.3.1 LAN TCP/IP 102
11.3.2 IP Alias 102
11.4 LAN IP Screen 102
11.5 IP Alias Screen 103

Chapter 12
Maintenance 105

12.1 Overview 105
12.2 What You Can Do 105
12.3 General Screen 105
12.4 Password Screen 106
12.5 Time Setting Screen 107
12.6 Firmware Upgrade Screen 109
12.7 Configuration Backup/Restore Screen 110
12.8 Reset/Restart Screen 111
12.9 System Operation Mode Overview 112
12.10 Sys Op Mode Screen 113

Chapter 13
Troubleshooting 115

13.1 Power, Hardware Connections, and LEDs 115
13.2 WAP3205 Access and Login 116
13.3 Internet Access 117
13.4 Resetting the WAP3205 to Its Factory Defaults 118
13.5 Wireless Router/AP Troubleshooting 119

Appendix A Pop-up Windows, JavaScripts and Java Permissions 121

Appendix B IP Addresses and Subnetting 131

Appendix C Setting Up Your Computer's IP Address 141

Appendix D Wireless LANs 169

Appendix E Common Services 183

Appendix F Legal Information 187

Index 193

PART I
User's Guide

1

Getting to Know Your WAP3205

1.1 Overview

This chapter introduces the main features and applications of the WAP3205.

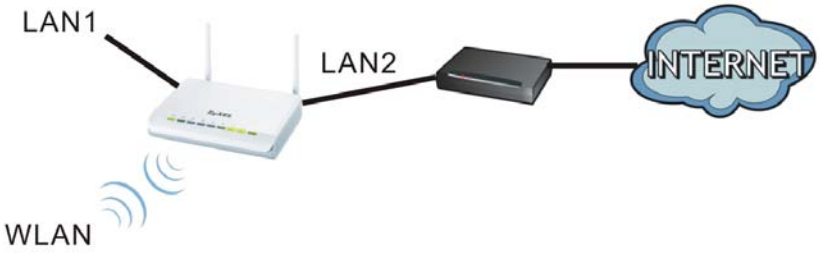
The WAP3205 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

1.2 Applications

Your can have the following networks on the WAP3205:

- **Wired**. You can connect to a broadband modem/router for Internet access and/or connect network devices via the Ethernet ports of the WAP3205 so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the WAP3205 to access network resources.

Figure 1 WAP3205 Network



1.3 Ways to Manage the WAP3205

Use any of the following methods to manage the WAP3205.

- Web Configurator. This is recommended for everyday management of the WAP3205 using a (supported) web browser.
- WPS (Wi-Fi Protected Setup) button. You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your WAP3205.

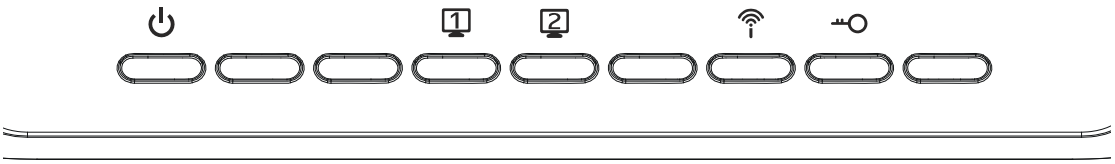
1.4 Good Habits for Managing the WAP3205

Do the following things regularly to make the WAP3205 more secure and to manage the WAP3205 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the WAP3205 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WAP3205. You could simply restore your last configuration.

1.5 LEDs

Figure 2 Front Panel



The following table describes the LEDs and the WPS button.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The WAP3205 is receiving power and functioning properly.
		Off	The WAP3205 is not receiving power.
LAN 1-2	Green	On	The WAP3205 has a successful 10/100MB Ethernet connection.
		Blinking	The WAP3205 is sending/receiving data through the LAN.
		Off	The LAN is not connected.
WLAN	Green	On	The WAP3205 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The WAP3205 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
WPS	Green	On	WPS is enabled.
		Blinking	The WAP3205 is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.

1.6 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes	12 cm
M4 Screws	Two
Screw anchors (optional)	Two

1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

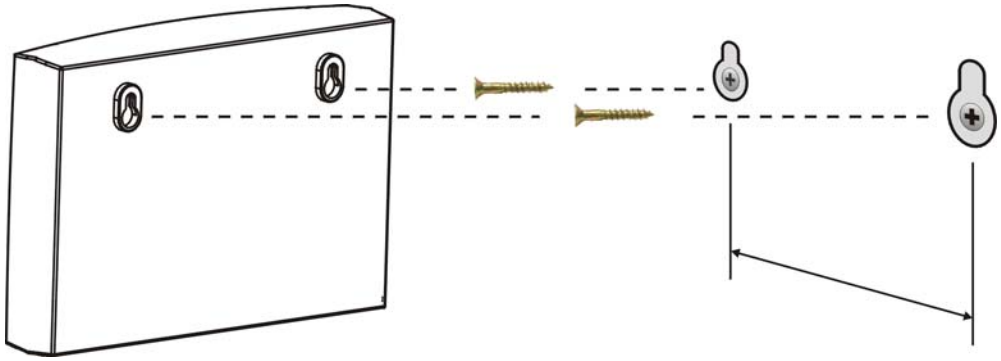
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the WAP3205 with the connection cables.

5 Align the holes on the back of the WAP3205 with the screws on the wall. Hang the WAP3205 on the screws.

Figure 3 Wall Mounting Example



2

WAP3205 Modes

2.1 Overview

This chapter introduces the different modes available on your WAP3205.

- **Device mode**. This is the operating mode of your WAP3205, or simply how the WAP3205 is being used in the network.

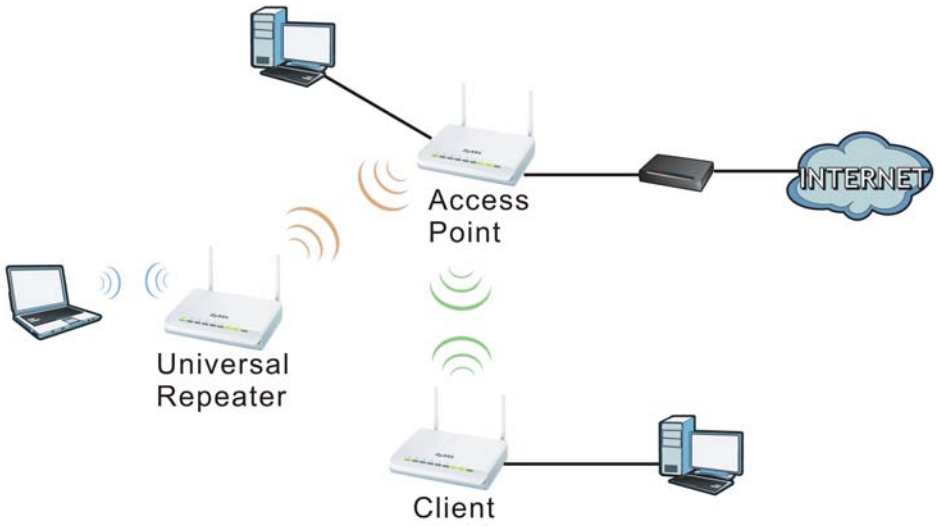
2.1.1 Device Modes

This refers to the operating mode of the WAP3205, which can act as a:

- **Access Point**. Use this mode if you want to extend your network by allowing network devices to connect to the WAP3205 wirelessly. Go to Section 3.4 on page 18 to view the **Status** screen in this mode.
- **Client**. Use this mode if there is an existing wireless router or access point in the network to which you want to connect your local network. Go to Section 4.5 on page 24 to view the **Status** screen in this mode. In Client mode, you should know the SSID and wireless security details of the access point to which you want to connect.
- **Universal Repeater**. In this mode, the WAP3205 can be an access point and a wireless client at the same time. Use this mode if there is an existing wireless router or access point in your network and you also want to allow clients to connect to the WAP3205 wirelessly. Go to Section 4.5 on page 24 to view the **Status** screen in this mode.

The following figure is a simple illustration of the device configuration modes of the WAP3205.

Figure 4 Device Mode Example



For more information on these modes and to change the mode of your WAP3205, refer to Chapter 12 on page 112.

Note: Choose your device mode carefully to avoid having to change it later.

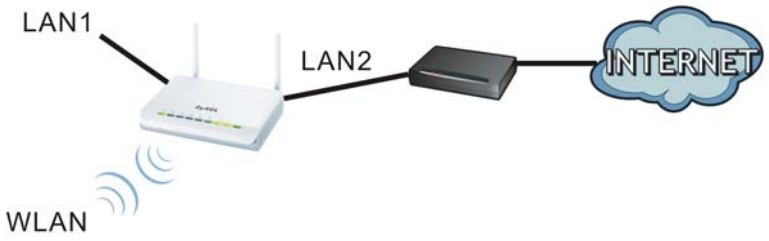
3

Access Point Mode

3.1 Overview

The WAP3205 is set to access point mode by default. In this mode your WAP3205 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 5 Wireless Internet Access in Access Point Mode



Note: See Chapter 8 on page 59 for an example of setting up a wireless network in Access Point mode.

3.2 What You Can Do

- Use the **Status** screen (Section 3.4 on page 18) to view read-only information about your WAP3205.
- Use the **LAN** screen (Chapter 11 on page 101) to set the IP address for your WAP3205 acting as an access point.
- Use the **Wireless LAN** screens (Chapter 10 on page 85) to configure the wireless settings and wireless security between the wireless clients and the WAP3205.

3.3 What You Need to Know

See Chapter 8 on page 59 for a tutorial on setting up a network with the WAP3205 as an access point.

3.3.1 Setting your WAP3205 to AP Mode

1. Connect your computer to the LAN port of the WAP3205.
2. The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 141 for information on changing your computer's IP address.

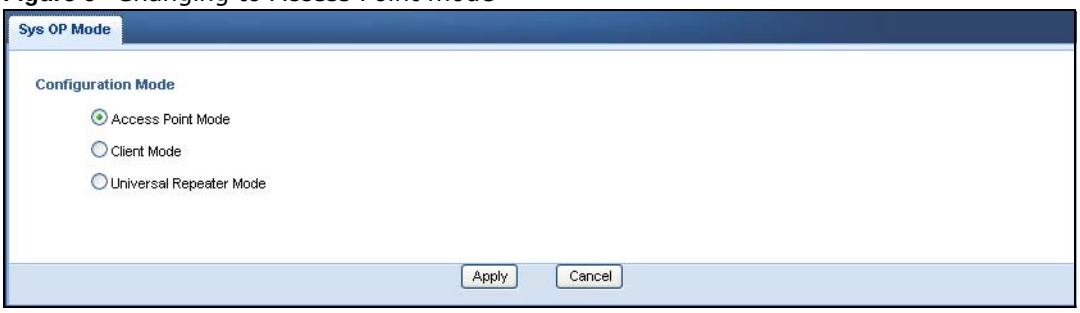
4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

5 Enter "1234" (default) as the password and click **Login**.

6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

7 To use your WAP3205 as an access point, on the left of the screen, click **Maintenance > Sys OP Mode** and select **Access Point Mode**. Click **Apply**.

Figure 6 Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your WAP3205 is already in access point mode.

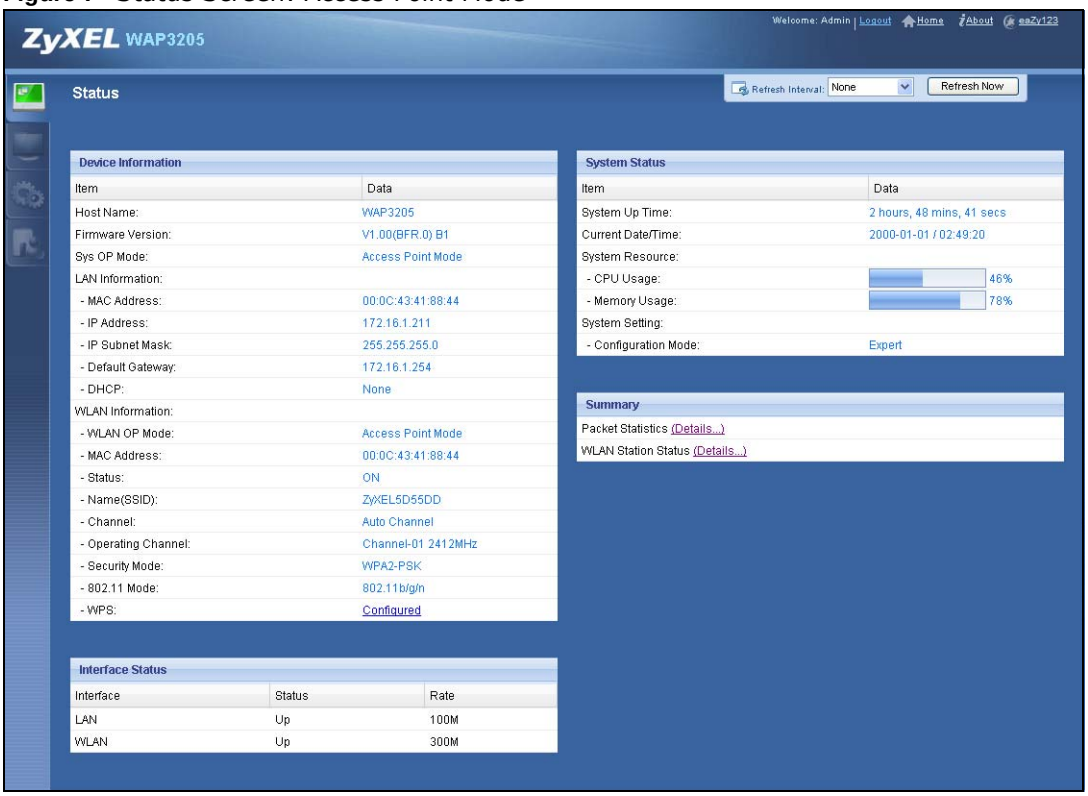
3.3.2 Configuring your WLAN, LAN and Maintenance Settings

- See Chapter 10 on page 85 and Chapter 11 on page 101 for information on the configuring your wireless network and LAN settings.
- See Chapter 12 on page 105 for information on configuring your Maintenance settings.

3.4 AP Mode Status Screen

Click to open the **Status** screen.

Figure 7 Status Screen: Access Point Mode



The following table describes the icons shown in the **Status** screen.

Table 3 Status Screen Icon Key: Access Point Mode

ICON	DESCRIPTION
Home	Click this to go to the Home page.
About	Click this icon to view copyright and a link for related product information.
easyZy123	Click this icon to open the wizard. See Chapter 7 on page 49.
Refresh Interval: None	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the **Monitor** navigation menu.
	Click this icon to see the **Configuration** navigation menu.
	Click this icon to see the **Maintenance** navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 4 Status Screen: Access Point Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the WAP3205's model name.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 2.1.1 on page 15) to which the WAP3205 is set - **Access Point Mode**.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
Default Gateway	This shows the gateway IP address.
DHCP	This shows the LAN port's DHCP role - **Client** or **None.**
WLAN Information	
WLAN OP Mode	This is the device mode (Section 2.1.1 on page 15) to which the WAP3205's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the wireless adapter MAC Address of your device.
Status	This shows the current status of the Wireless LAN - **ON**.
Name (SSID)	This shows a descriptive name used to identify the WAP3205 in the wireless LAN.
Channel	This shows the channel number which you select manually or the WAP3205 automatically scans and selects.
Operating Channel	This shows the channel number which the WAP3205 is currently using over the wireless LAN.
Security Mode	This shows the level of wireless security the WAP3205 is using.
802.11 Mode	This shows the wireless standard.
WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up. Click the status to display **Network > Wireless LAN > WPS** screen.
Interface Status	
Interface	This displays the WAP3205 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
System Status	
Item	This column shows the type of data the WAP3205 is recording.
Data	This column shows the actual data recorded by the WAP3205.
System Up Time	This is the total time the WAP3205 has been on.
Current Date/Time	This field displays your WAP3205's present date and time.

Table 4 Status Screen: Access Point Mode

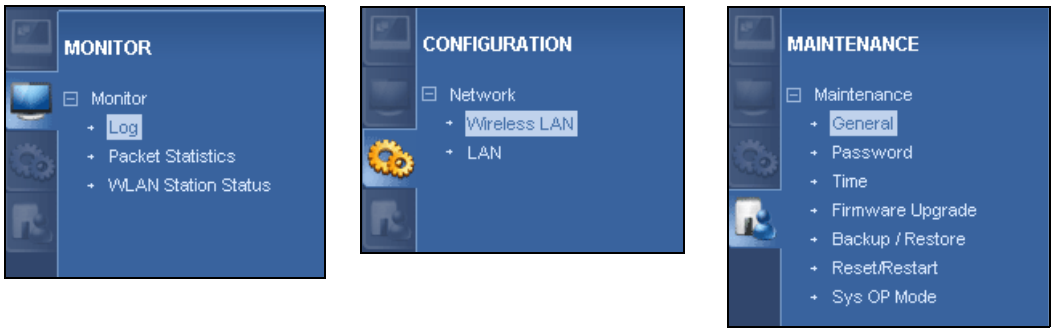
LABEL	DESCRIPTION
System Resource	
CPU Usage	This displays what percentage of the WAP3205's processing ability is currently used. When this percentage is close to 100%, the WAP3205 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
Memory Usage	This shows what percentage of the heap memory the WAP3205 is using.
System Setting	
Configuration Mode	This shows the web configurator mode you are viewing - **Expert**.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 9.4 on page 82). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN Station Status** screen (Section 9.5 on page 83). Use this screen to view the wireless stations that are currently associated to the WAP3205.

3.4.0.1 Navigation Panel

Use the menu in the navigation panel to configure WAP3205 features in Access Point mode.

The following screen and table show the features you can configure in Access Point mode.

Figure 8 Menu: Access Point Mode



The following table describes the sub-menus.

Table 5 Navigation Panel: Access Point Mode

LINK	TAB	FUNCTION
Status		This screen shows the WAP3205's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
MONITOR		
Log		Use this screen to view the list of activities recorded by your WAP3205.
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the WAP3205.
CONFIGURATION		
Network		

Table 5 Navigation Panel: Access Point Mode

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure general wireless LAN settings.
	Security	Use this screen to configure wireless security settings.
	MAC Filter	Use the MAC filter screen to configure the WAP3205 to block access to devices or block the devices from accessing the WAP3205.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	WDS	Use this screen to set up Wireless Distribution System (WDS) on your WAP3205.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to have the WAP3205 apply IP alias to create LAN subnets.
MAINTENANCE		
General		Use this screen to view and change administrative settings such as system and domain names.
Password	Password Setup	Use this screen to change the password of your WAP3205.
Time	Time Setting	Use this screen to change your WAP3205's time and date.
Firmware Upgrade		Use this screen to upload firmware to your WAP3205.
Backup/ Restore		Use this screen to backup and restore the configuration or reset the factory defaults to your WAP3205.
Reset/ Restart	Restart	This screen allows you to reboot the WAP3205 without turning the power off.
Sys OP Mode		This screen allows you to select whether your device acts as an access point, wireless client or both at the same time.

4

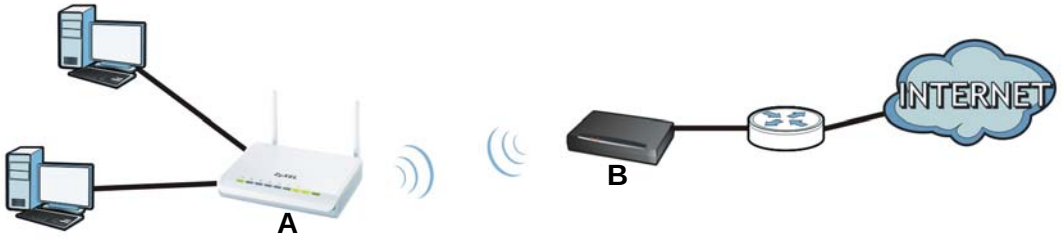
Client Mode

4.1 Overview

Your WAP3205 can act as a wireless client. In wireless client mode, it can connect to an existing network via an access point. Use this mode if you already have an access point or wireless router in your network.

In the example below, one WAP3205 (**A**) is configured as a wireless client and another is used as an access point (**B**). The WAP3205 has two clients that need to connect to the Internet. The WAP3205 wirelessly connects to the available access point (**B**).

Figure 9 Wireless Client Mode



After the WAP3205 and the access point connect, the WAP3205 acquires its WAN IP address from the access point. The clients of the WAP3205 can now surf the Internet.

4.2 What You Can Do

- Use the **Status** screen (Section 4.5 on page 24) to view read-only information about your WAP3205.
- Use the **LAN** screen (Chapter 11 on page 101) to set the IP address for your WAP3205.
- Use the **Wireless LAN** screen (Section 4.6 on page 26) to associate your WAP3205 (acting as a wireless client) with an existing access point.

4.3 What You Need to Know

With the exception of the **Wireless LAN** screens, the **LAN**, **Monitor**, **Configuration** and **Maintenance** screens in Client mode are similar to the ones in Access Point Mode. See Chapter 11 on page 101 through Chapter 12 on page 105 of this User's Guide.

4.4 Setting your WAP3205 to Client Mode

1 Connect your computer to the LAN port of the WAP3205.

2 The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 141 for information on changing your computer's IP address.

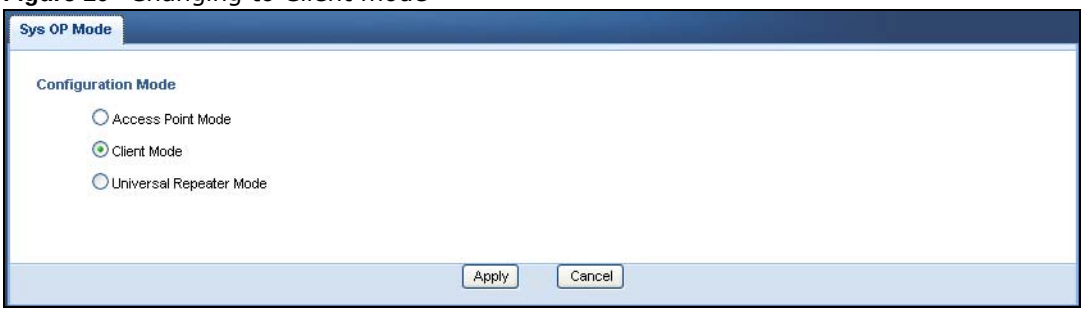
4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

5 Enter "1234" (default) as the password and click **Login**.

6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

7 To set your WAP3205 to **Client Mode**, on the left of the screen, click **Maintenance > Sys OP Mode** and select **Client Mode**.

Figure 10 Changing to Client mode



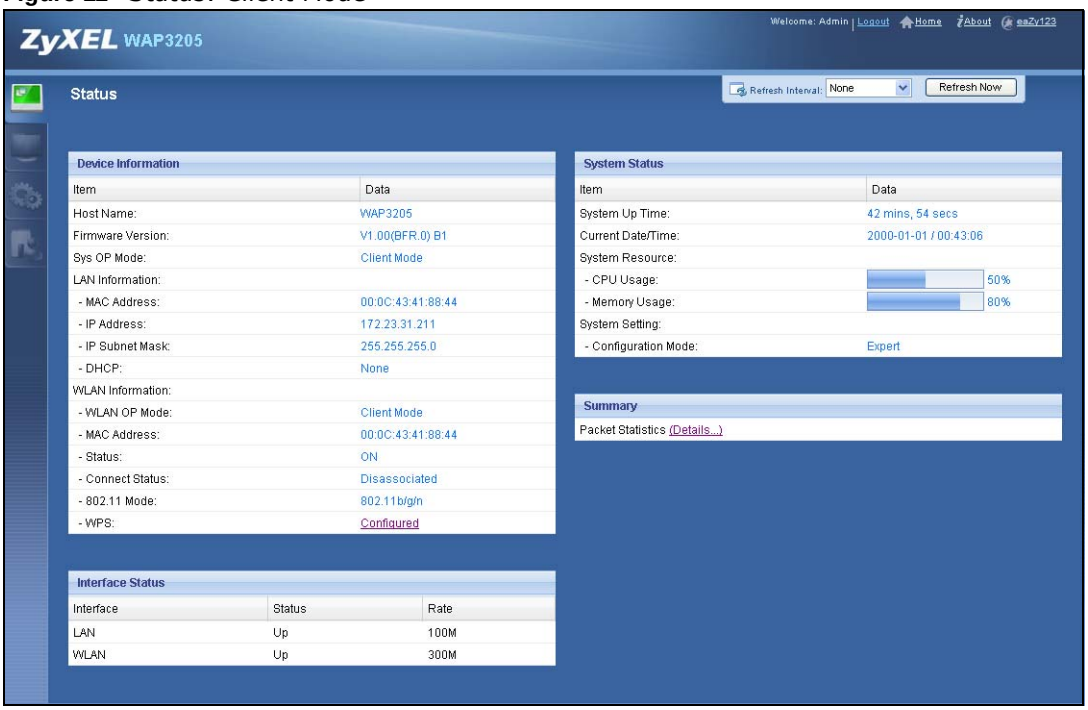
Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your WAP3205 is already in Client mode.

Note: The client mode IP address is always the same as the access point mode IP address. If you changed the IP address of your WAP3205 while in access point mode, use this IP address in client mode.

4.5 Client Mode Status Screen

Click to open the status screen.

Figure 11 Status: Client Mode



The following table describes the labels shown in the **Status** screen.

Table 6 Status Screen: Client Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the WAP3205's model name.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 2.1.1 on page 15) to which the WAP3205 is set - **Client Mode**.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - **Client** or **None**.
WLAN Information	
WLAN OP Mode	This is the device mode (Section 2.1.1 on page 15) to which the WAP3205's wireless LAN is set - **Client Mode**.
MAC Address	This shows the wireless adapter MAC Address of your device.
Status	This shows the current status of the Wireless LAN - **ON**.
Name (SSID)	This shows a descriptive name used to identify the WAP3205 in the wireless LAN.
Connect Status	This shows whether or not the WAP3205 has successfully associated with an access point - **Connected** or **Disassociated**.
802.11 Mode	This shows the wireless standard.

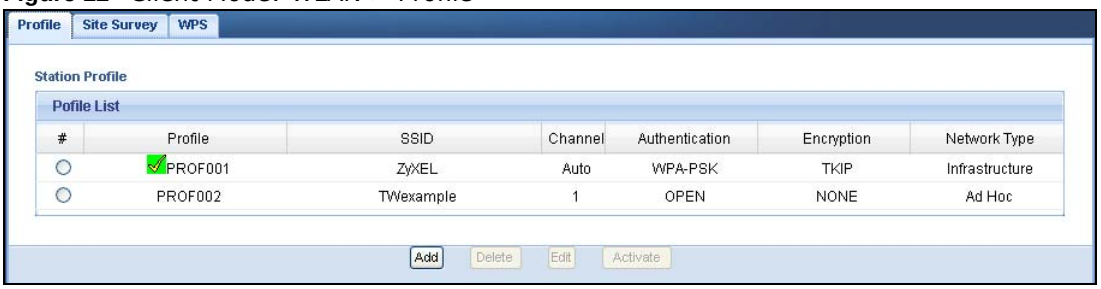
Table 6 Status Screen: Client Mode

LABEL	DESCRIPTION
WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up. Click the status to display **Network > Wireless LAN > WPS** screen.
Interface Status	
Interface	This displays the WAP3205 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
System Status	
Item	This column shows the type of data the WAP3205 is recording.
Data	This column shows the actual data recorded by the WAP3205.
System Up Time	This is the total time the WAP3205 has been on.
Current Date/Time	This field displays your WAP3205's present date and time.
System Resource	
CPU Usage	This displays what percentage of the WAP3205's processing ability is currently used. When this percentage is close to 100%, the WAP3205 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
Memory Usage	This shows what percentage of the heap memory the WAP3205 is using.
System Setting	
Configuration Mode	This shows the web configurator mode you are viewing - **Expert**.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 9.4 on page 82). Use this screen to view port status and packet specific statistics.

4.6 Wireless LAN Profile Screen

Use this screen to view the wireless LAN profile settings of your WAP3205. Go to **Configuration > Wireless LAN > Profile** to open the following screen.

Figure 12 Client Mode: WLAN > Profile



The following table describes the labels in this screen.

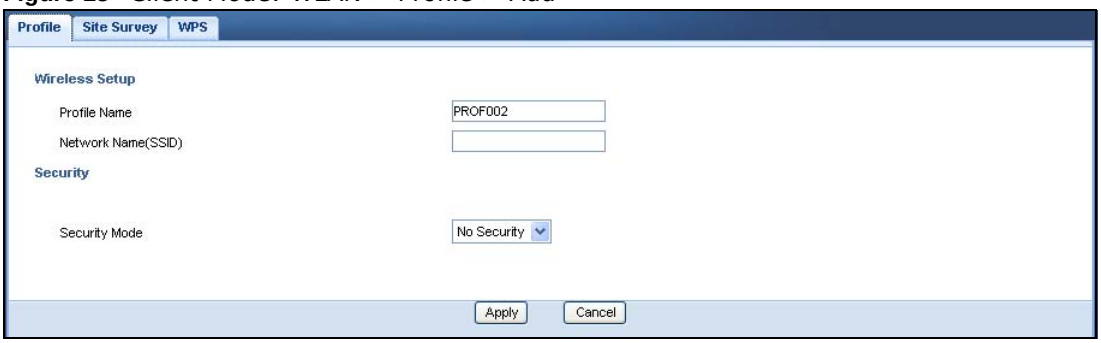
Table 7 Client Mode: WLAN > Profile

LABEL	DESCRIPTION
Profile List	
#	Select a profile to remove, modify or enable it.
Profile	This displays the name of the pre-configured profile. indicates the profile is activated and the WAP3205 connects to the specified wireless network. indicates the profile is activated but the specified wireless network is not available or the WAP3205 fails to associate with the wireless network.
SSID	This displays the SSID of the wireless network with which this profile associates.
Channel	This displays the channel number used by this profile. **Auto** means the WAP3205 automatically scans for and selects an available channel.
Authentication	This displays the authentication method used by this profile.
Encryption	This displays the data encryption method used by this profile.
Network Type	This displays the network type (**Infrastructure** or **Ad Hoc**) of this profile.
Add	Click this button to create a new profile.
Delete	Select a profile and click this button to remove it.
Edit	Select a profile and click this button to modify it.
Activate	Select a profile and click this button to enable it. Note: You can activate only one profile at a time.

4.6.1 Adding a New WLAN Profile

Use this screen to create a new wireless LAN profile for your WAP3205. Click the **Add** button in the **Configuration > Wireless LAN > Profile** screen to open the following screen.

Figure 13 Client Mode: WLAN > Profile > Add



The following table describes the labels in this screen.

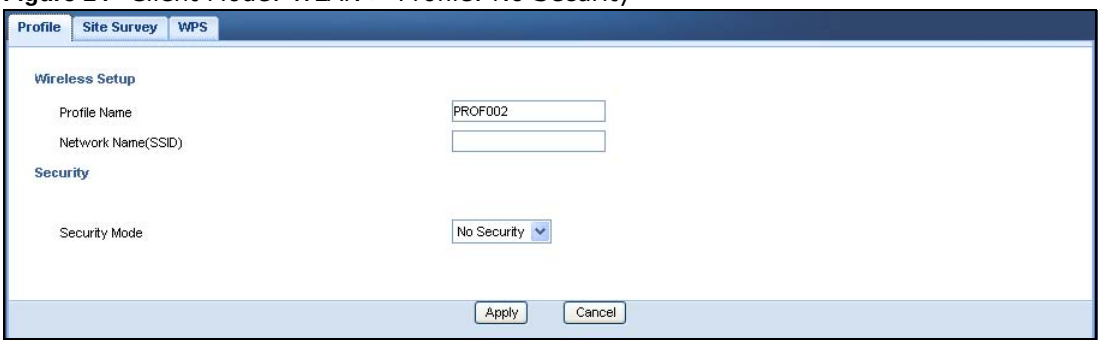
Table 8 Client Mode: WLAN > Profile > Add

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select the security mode of the access point to which you want to connect.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to go back to the previous screen.

4.6.1.1 No Security

Use this screen if the access point to which you want to connect does not use encryption.

Figure 14 Client Mode: WLAN > Profile: No Security



The following table describes the labels in this screen.

Table 9 Client Mode: WLAN > Profile: No Security

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select **No Security** in this field.

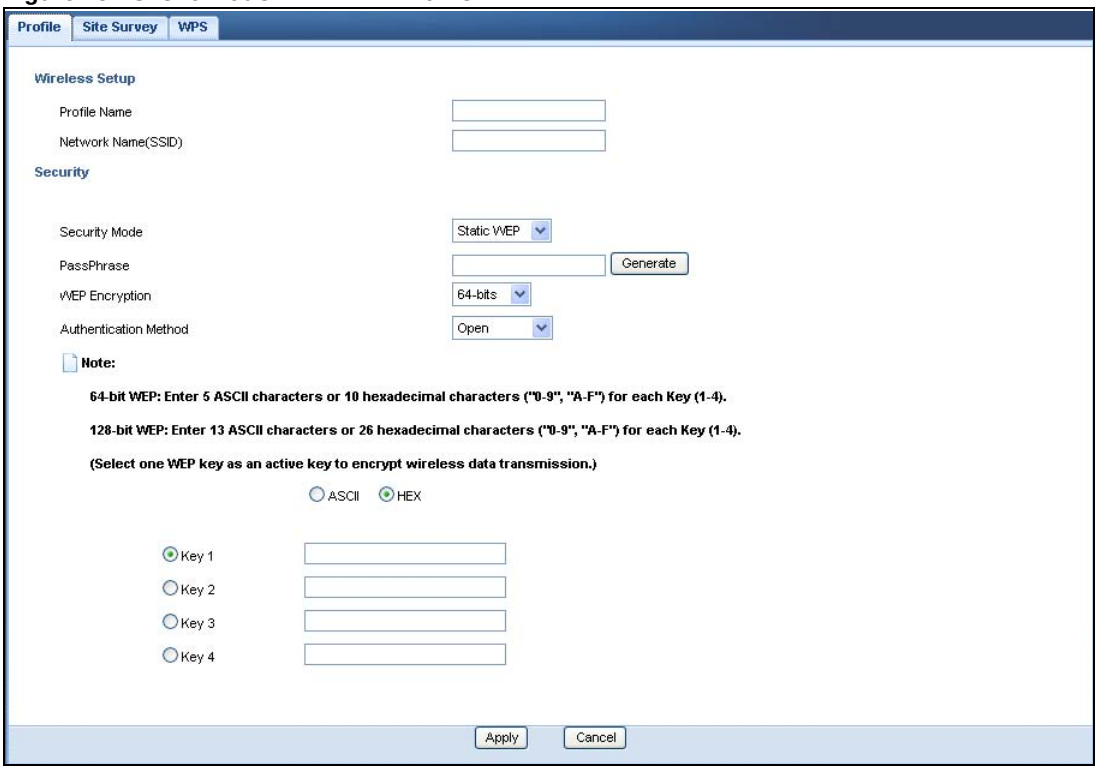
Table 9 Client Mode: WLAN > Profile: No Security (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to go back to the previous screen.

4.6.1.2 Static WEP

Use this screen if the access point to which you want to connect to uses WEP security mode.

Figure 15 Client Mode: WLAN > Profile: WEP



The following table describes the labels in this screen..

Table 10 Client Mode: WLAN > Profile: WEP

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select **Static WEP** to enable data encryption.
PassPhrase	Enter a passphrase (up to 26 printable characters) and click **Generate**. A passphrase functions like a password. In WEP security mode, it is further converted by the WAP3205 into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.

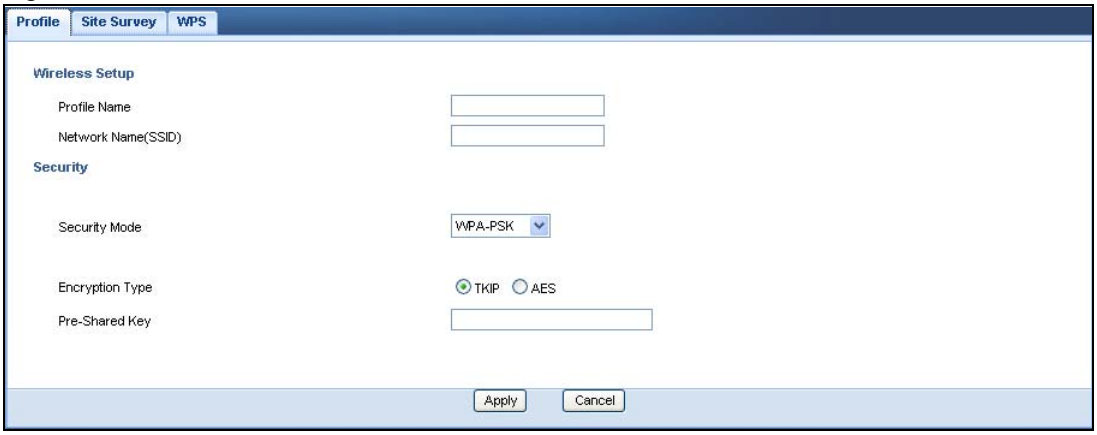
Table 10 Client Mode: WLAN > Profile: WEP

LABEL	DESCRIPTION
WEP Encryption	Select **64-bit WEP** or **128-bit WEP**. This dictates the length of the security key that the network is going to use.
Authentication Method	Select **Open** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to log into the wireless network. Keep this setting at **Open** unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the WAP3205 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to go back to the previous screen.

4.6.1.3 WPA(2)-PSK

Use this screen if the access point to which you want to connect uses WPA(2)-PSK security mode.

Figure 16 Client Mode: WLAN > Profile: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen. .

Table 11 Client Mode: WLAN > Profile: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Wireless Setup	
Profile Name	Enter a descriptive name for this profile.

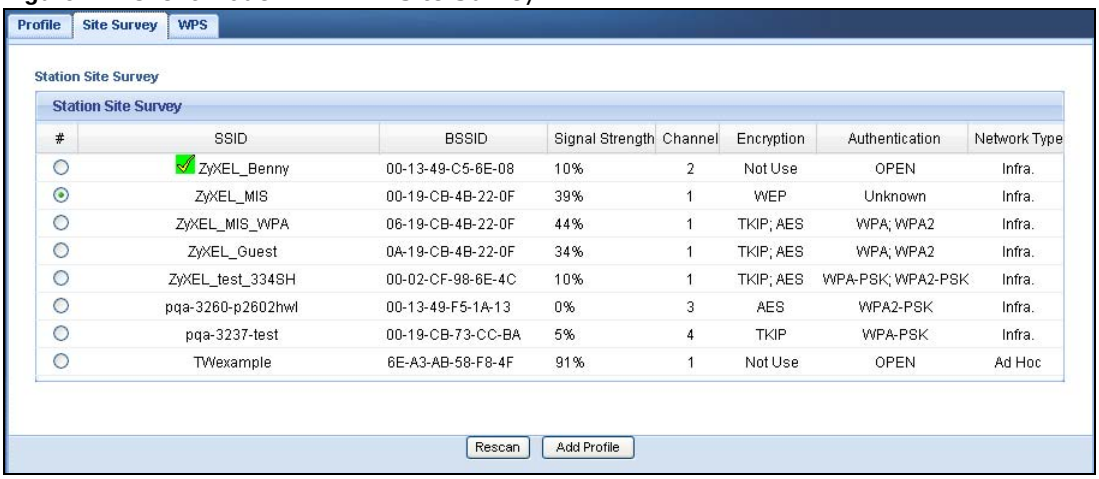
Table 11 Client Mode: WLAN > Profile: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Network Name (SSID)	Enter the name of the access point to which you are connecting.
Security	
Security Mode	Select **WPA-PSK** or **WPA2-PSK** to add strong security on this wireless network.
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	**WPA-PSK** or **WPA2-PSK** uses a simple common password for authentication. Type the pre-shared key employed by the access point to which you want to connect.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to go back to the previous screen.

4.7 Site Survey Screen

Use this screen to scan for and connect to a wireless network automatically. Go to **Configuration > Wireless LAN > Site Survey** to open the following screen.

Figure 17 Client Mode: WLAN > Site Survey



The following table describes the labels in this screen.

Table 12 Client Mode: WLAN > Site Survey

LABEL	DESCRIPTION
Station Site Survey	
#	Select a wireless device and click **Add Profile** to open a configuration screen where you can add the selected wireless device to a profile and then enable it.
SSID	This displays the SSID of the wireless device. indicates the wireless device is added to an activated profile and the WAP3205 is connecting to it.
BSSID	This displays the MAC address of the wireless device.

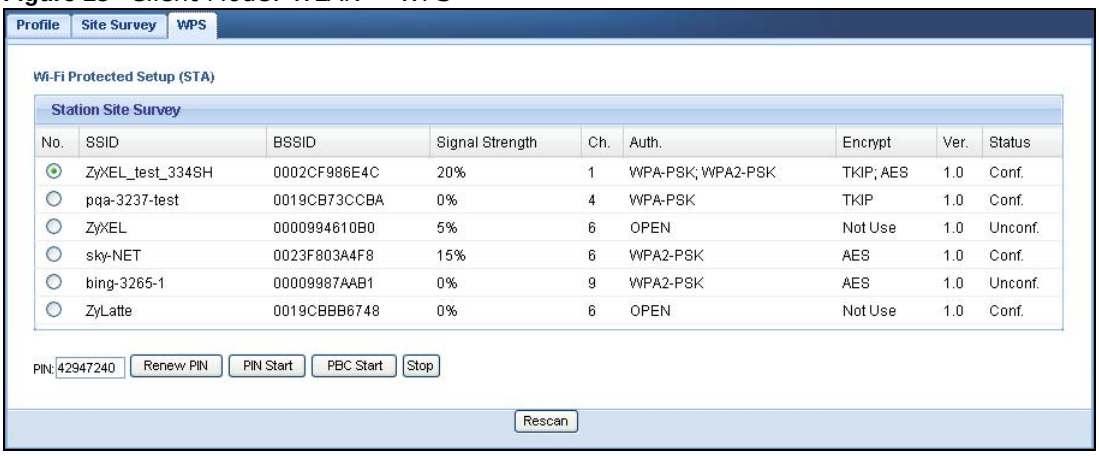
Table 12 Client Mode: WLAN > Site Survey (continued)

LABEL	DESCRIPTION
Signal Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your WAP3205 and this device.
Channel	This displays the channel number used by this wireless device.
Encryption	This displays the data encryption method used by this wireless device.
Authentication	This displays the authentication method used by this wireless device.
Network Type	This displays the network type (**Infrastructure** or **Ad Hoc**) of this wireless device.
Rescan	Click this button to search for available wireless devices within transmission range and update this table.
Add Profile	Select a wireless device and click this button to add it to a profile.

4.8 WPS Screen

Use this screen to enable Wi-Fi Protected Setup (WPS) on the WAP3205. Go to **Configuration > Wireless LAN > WPS** to open the following screen.

Figure 18 Client Mode: WLAN > WPS



The following table describes the labels in this screen.

Table 13 Client Mode: WLAN > WPS

LABEL	DESCRIPTION
Station Site Survey	
#	Use the radio button to select the wireless device to which you want to connect using WPS.
SSID	This displays the SSID of the wireless device.
BSSID	This displays the MAC address of the wireless device.
Signal Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your WAP3205 and this device.
Ch.	This displays the channel number used by this wireless device.
Auth.	This displays the authentication method used by this wireless device.

Table 13 Client Mode: WLAN > WPS (continued)

LABEL	DESCRIPTION
Encrypt	This displays the data encryption method used by this wireless device.
Ver.	This displays the firmware version running on the wireless device.
Status	This displays **Conf.** (configured) when WPS has been set up on the wireless device. This displays **Unconf.** (unconfigured) if WPS has not been set up on the wireless device.
PIN	This displays the PIN number of the WAP3205.
Renew PIN	Click this button to generate a new PIN and display it in the **PIN** field.
PIN Start	Click this button to perform wireless security information synchronization using the PIN configuration method.
PBC Start	Click this button to perform wireless security information synchronization using the Push Button Configuration (PBC) method.
Stop	Click this button to cancel wireless security information synchronization.
Rescan	Click this button to search for available for WPS-enabled devices within transmission range and update this table.

5

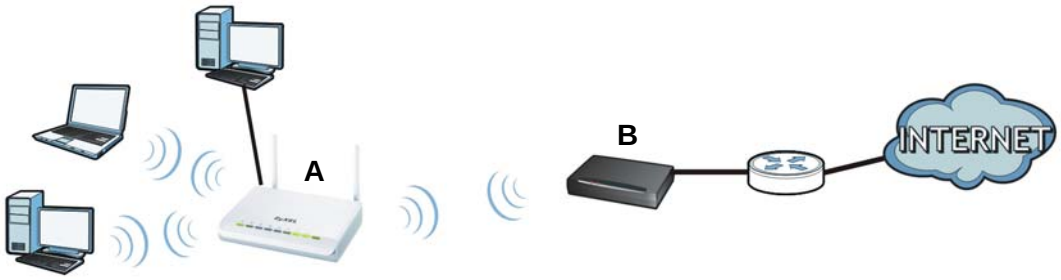
Universal Repeater Mode

5.1 Overview

In universal repeater mode, your WAP3205 can act as an access point and wireless client at the same time. The WAP3205 can connect to an existing network through another access point and also lets wireless clients connect to the network through it. This helps you expand wireless coverage when you have an access point or wireless router already in your network.

In the example below, the WAP3205 (**A**) is configured as a universal repeater. It has three clients that want to connect to the Internet. The WAP3205 wirelessly connects to the available access point (**B**).

Figure 19 Universal Repeater Mode



After the WAP3205 and the access point connect, the WAP3205 acquires its IP address from the access point. The clients of the WAP3205 can now surf the Internet.

5.2 What You Can Do

- Use the **Status** screen (Section 4.5 on page 24) to view read-only information about your WAP3205.
- Use the **LAN** screen (Chapter 11 on page 101) to set the IP address for your WAP3205.
- Use the **Wireless LAN > Universal Repeater** screen (Section 4.6 on page 26) to configure the security between the WAP3205 and another access point.
- Use other **Wireless LAN** screens (Chapter 10 on page 85) to configure the wireless settings and wireless security between the wireless clients and the WAP3205.

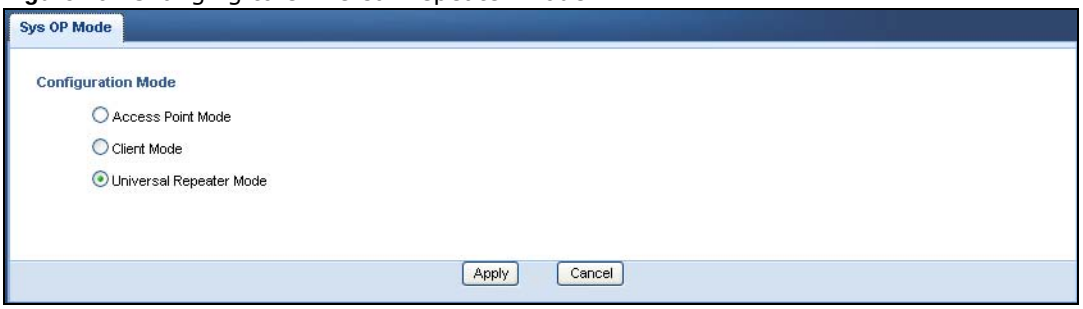
5.3 What You Need to Know

With the exception of the **Wireless LAN > Universal Repeater** screen, other configuration screens in Universal Repeater mode are similar to the ones in Access Point Mode. See Chapter 11 on page 101 through Chapter 12 on page 105 of this User's Guide.

5.4 Setting your WAP3205 to Universal Repeater Mode

1. Connect your computer to the LAN port of the WAP3205.
2. The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
3. Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 141 for information on changing your computer's IP address.
4. After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.
5. Enter "1234" (default) as the password and click **Login**.
6. Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.
7. To set your WAP3205 to **Universal Repeater Mode**, on the left of the screen, click **Maintenance > Sys OP Mode** and select **Universal Repeater Mode**.

Figure 20 Changing to Universal Repeater mode



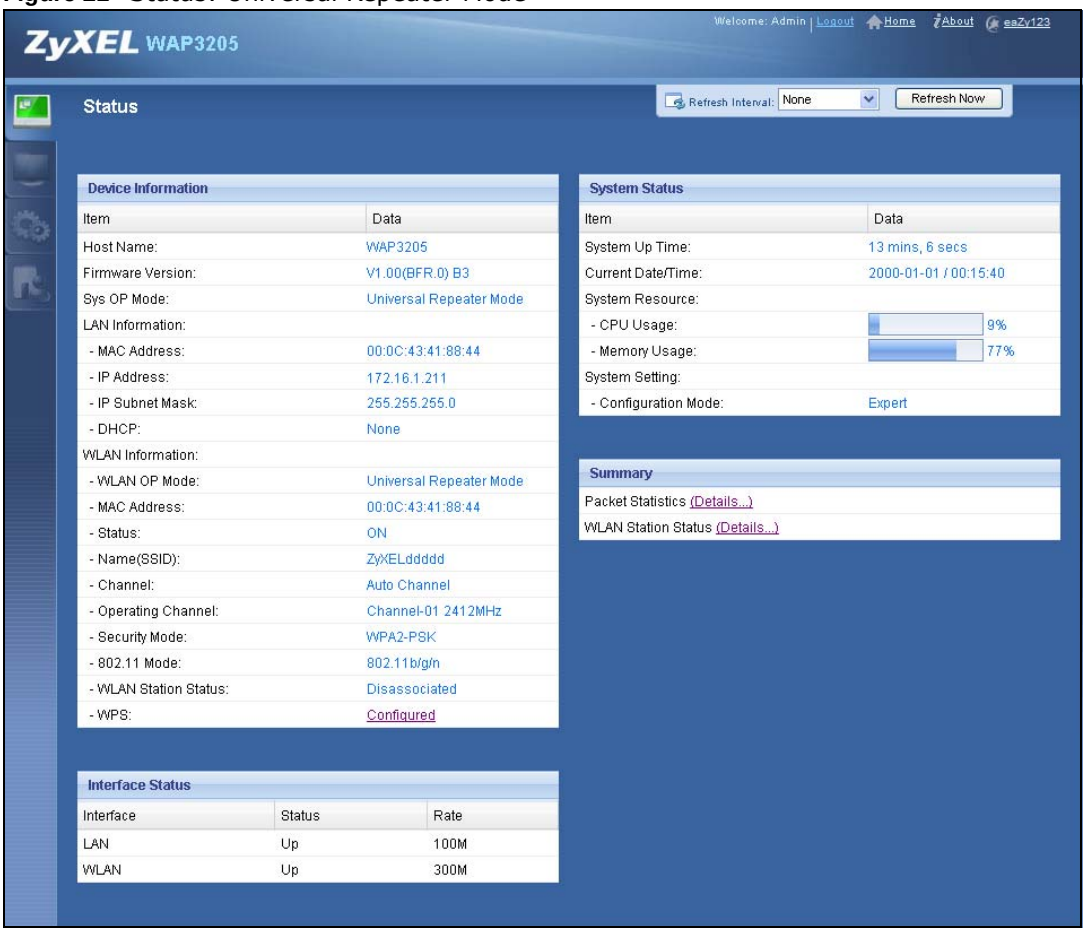
Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your WAP3205 is already in Universal Repeater mode.

Note: The universal repeater mode IP address is always the same as the access point mode IP address. If you changed the IP address of your WAP3205 while in access point mode, use this IP address in universal repeater mode.

5.5 Universal Repeater Mode Status Screen

Click to open the status screen.

Figure 21 Status: Universal Repeater Mode



The following table describes the labels shown in the **Status** screen.

Table 14 Status Screen: Universal Repeater Mode

LABEL	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
Device Information	
Host Name	This is the WAP3205's model name.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 2.1.1 on page 15) to which the WAP3205 is set - **Universal Repeater Mode**.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - **Client** or **None**.
WLAN Information	
WLAN OP Mode	This is the device mode (Section 2.1.1 on page 15) to which the WAP3205's wireless LAN is set - **Universal Repeater Mode**.
MAC Address	This shows the wireless adapter MAC Address of your device.
Status	This shows the current status of the Wireless LAN - **ON**.

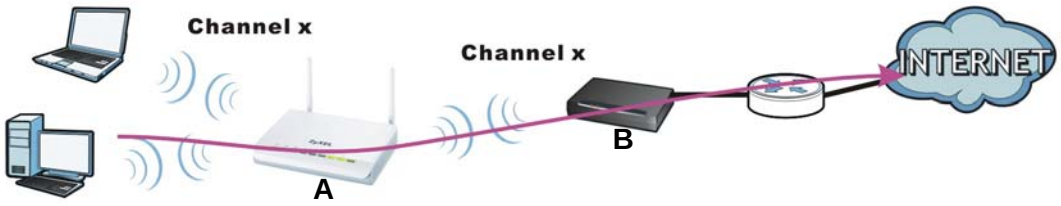
Table 14 Status Screen: Universal Repeater Mode

LABEL	DESCRIPTION
Name (SSID)	This shows a descriptive name used to identify the WAP3205 in the wireless LAN.
Channel	This shows the channel number which you select manually or the WAP3205 automatically scans and selects.
Operating Channel	This shows the channel number which the WAP3205 is currently using over the wireless LAN.
Security Mode	This shows the level of wireless security the WAP3205 is using.
802.11 Mode	This shows the wireless standard.
WLAN Station Status	This shows the SSID and MAC address of the AP or wireless router with which the WAP3205 is currently associated. Otherwise, it displays **Disassociated**.
WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up. Click the status to display **Network > Wireless LAN > WPS** screen.
Interface Status	
Interface	This displays the WAP3205 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
System Status	
Item	This column shows the type of data the WAP3205 is recording.
Data	This column shows the actual data recorded by the WAP3205.
System Up Time	This is the total time the WAP3205 has been on.
Current Date/Time	This field displays your WAP3205's present date and time.
System Resource	
CPU Usage	This displays what percentage of the WAP3205's processing ability is currently used. When this percentage is close to 100%, the WAP3205 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
Memory Usage	This shows what percentage of the heap memory the WAP3205 is using.
System Setting	
Configuration Mode	This shows the web configurator mode you are viewing - **Expert**.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 9.4 on page 82). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN Station Status** screen (Section 9.5 on page 83). Use this screen to view the wireless stations that are currently associated to the WAP3205.

5.6 Universal Repeater Screen

Use this screen to enter the SSID and select the wireless security mode used by the wireless device to which you want to connect. Go to **Configuration > Wireless LAN > Universal Repeater** to open the **Universal Repeater** screen. The screen varies depending on security mode.

Note: To have wireless clients access or acquire an IP address from another access point or wireless router (**B**) through the WAP3205 (**A**) in universal repeater mode, you must set the channel number in the **Wireless LAN > General** screen to be the same as the one on the wireless router or AP to which the WAP3205 wants to connect.



5.6.1 No Security

Figure 22 Universal Repeater Mode: Wireless LAN > Universal Repeater: No Security

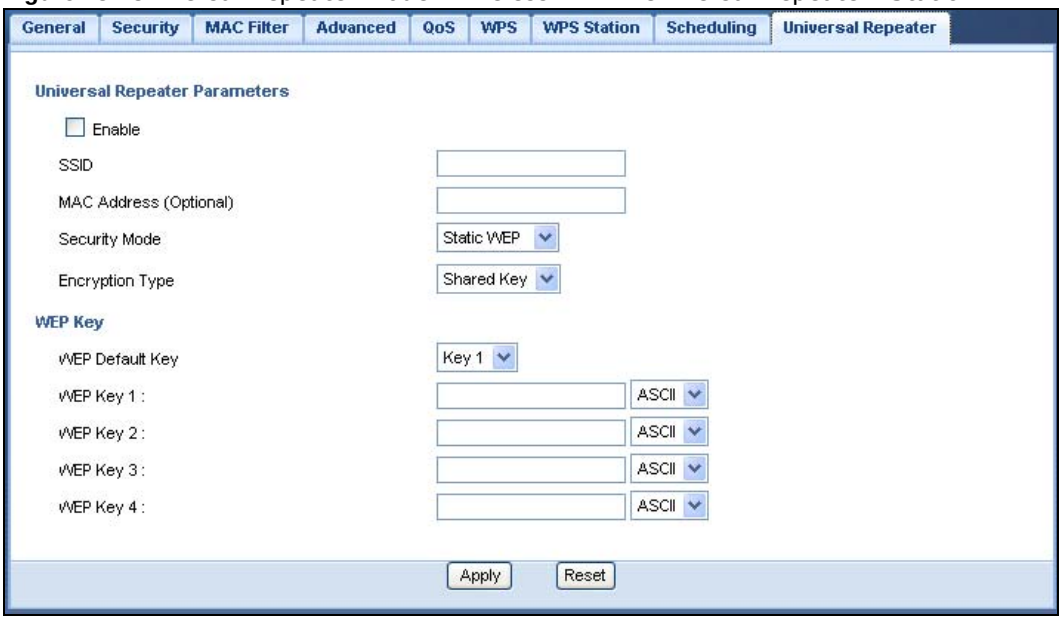
The following table describes the labels in this screen.

Table 15 Universal Repeater Mode: Wireless LAN > Universal Repeater: No Security

LABEL	DESCRIPTION
Universal Repeater Parameters	
Enable	Select this option to have the WAP3205 connect to the specified access point.
SSID	Enter the name of the access point to which you are connecting.
MAC Address (Optional)	Enter the MAC address of the access point to which you are connecting.
Security Mode	Select **No Security** if the access point to which you want to connect does not use encryption.
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.6.2 Static WEP

Figure 23 Universal Repeater Mode: Wireless LAN > Universal Repeater: Static WEP



The following table describes the labels in this screen.

Table 16 Universal Repeater Mode: Wireless LAN > Universal Repeater: Static WEP

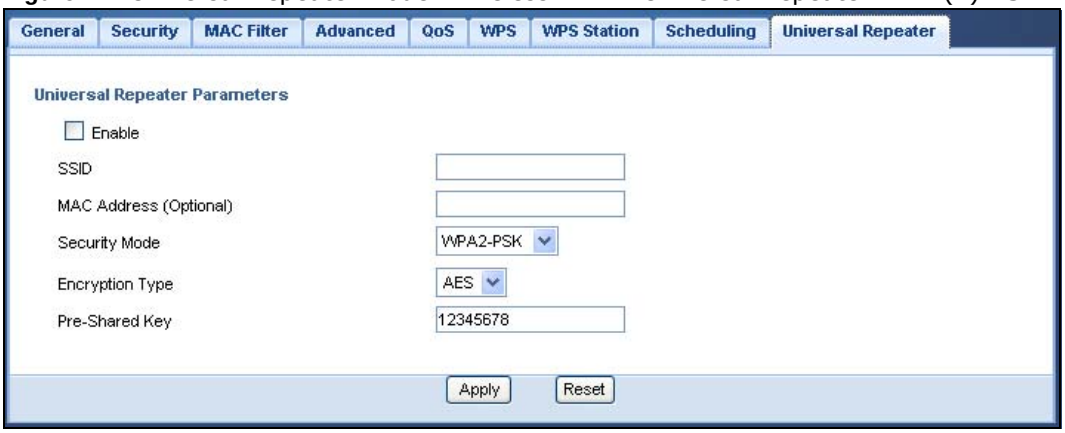
LABEL	DESCRIPTION
Universal Repeater Parameters	
Enable	Select this option to have the WAP3205 connect to the specified access point.
SSID	Enter the name of the access point to which you are connecting.
MAC Address (Optional)	Enter the MAC address of the access point to which you are connecting.
Security Mode	Select **Static WEP** if the access point to which you want to connect uses WEP data encryption.
Encryption Type	Select **Open** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to log into the wireless network. Keep this setting at **Open** unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
WEP Key	
WEP Default Key	Select a default WEP key to use for data encryption.

Table 16 Universal Repeater Mode: Wireless LAN > Universal Repeater: Static WEP

LABEL	DESCRIPTION
WEP Key 1 ~ WEP Key 4	The WEP keys are used to encrypt data. Both the WAP3205 and the access point must use the same WEP key for data transmission. If you chose **HEX**, enter 10 or 26 hexadecimal characters in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for a 64-bit or 128-bit WEP key respectively. If you chose **ASCII**, enter any 5 or 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for a 64-bit or 128-bit WEP key respectively. You must configure at least one key, only one key can be activated at any one time.
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.6.3 WPA(2)-PSK

Figure 24 Universal Repeater Mode: Wireless LAN > Universal Repeater: WPA(2)-PSK



The following table describes the labels in this screen.

Table 17 Universal Repeater Mode: Wireless LAN > Universal Repeater: WPA(2)-PSK

LABEL	DESCRIPTION
Universal Repeater Parameters	
Enable	Select this option to have the WAP3205 connect to the specified access point.
SSID	Enter the name of the access point to which you are connecting.
MAC Address (Optional)	Enter the MAC address of the access point to which you are connecting.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** if the access point to which you want to connect uses WPA-PSK or WPA2-PSK.
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	**WPA-PSK** or **WPA2-PSK** uses a simple common password for authentication. Type the password employed by the access point to which you want to connect.
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to reload the previous configuration for this screen.

6

Introducing the Web Configurator

6.1 Overview

This chapter describes how to access the WAP3205 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the WAP3205 via Internet browser. Use Internet Explorer 6.0 and later or Safari 2.0 or later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 13 on page 115) to see how to make sure these functions are allowed in Internet Explorer.

6.2 Accessing the Web Configurator

1. Connect your computer to the LAN port of the WAP3205.
2. The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
3. Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 141 for information on changing your computer's IP address.
4. After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

6.2.1 Login Screen

The Web Configurator initially displays the following login screen.

Figure 25 Login screen

The following table describes the labels in this screen.

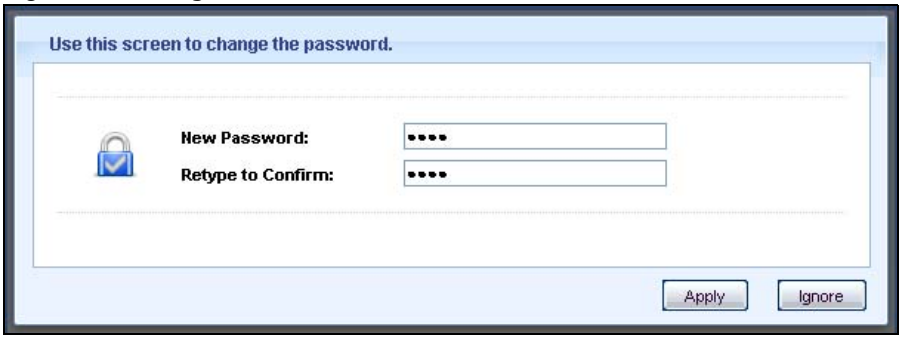
Table 18 Login screen

LABEL	DESCRIPTION
Password	Type "1234" (default) as the password.
Language	Select the language you want to use to configure the Web Configurator. Click **Login**.
	This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 6.2.3.1 on page 46.
	This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 6.2.3.2 on page 46 or Section 12.5 on page 107. The time is in 24-hour format, for example 15:00 is 3:00 PM.

6.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 26 Change Password Screen



The following table describes the labels in this screen.

Table 19 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click **Apply** to save your changes back to the WAP3205.
Ignore	Click **Ignore** if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 12 on page 105 to change this). Simply log back into the WAP3205 if this happens.

6.2.3 Home Screen

If you have previously logged into the Web Configurator but did not click **Logout**, you may be redirected to the **Home** screen.

You can also open this screen by clicking **Home** (

) in the Web Configurator screens.

The Home screen displays as follows.

Figure 27 Home Screen

The following table describes the labels in this screen.

Table 20 Home Screen

LABEL	DESCRIPTION
Go	Click this to open the Web Configurator **Status** screen.
Language	Select a language to go to the Web Configurator in that language and click **Login**.

Table 20 Home Screen

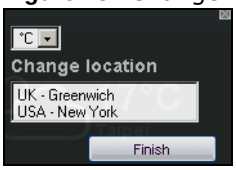
LABEL	DESCRIPTION
	(This is just an example). This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 6.2.3.1 on page 46.
	(This is just an example). This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 6.2.3.2 on page 46 or Section 12.5 on page 107.

6.2.3.1 Weather Edit

You can change the temperature unit and select the location for which you want to know the weather.

Click the icon to change the weather display.

Figure 28 Change Weather



The following table describes the labels in this screen.

Table 21 Change Weather

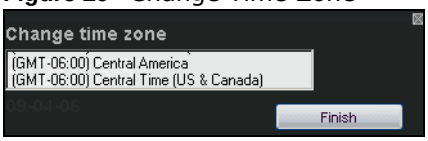
LABEL	DESCRIPTION
°C or °F	Choose which temperature unit you want the WAP3205 to display.
Change Location	Select the location for which you want to know the weather. If the city you want is not listed, choose one that is closest to it.
Finish	Click this to apply the settings and refresh the date and time display.

6.2.3.2 Time/Date Edit

One timezone can cover more than one country. You can choose a particular country in which the WAP3205 is located and have the WAP3205 display and use the current time and date for its logs.

Click the icon to change the time and date display.

Figure 29 Change Time Zone



The following table describes the labels in this screen.

Table 22 Change Time Zone

LABEL	DESCRIPTION
Change time zone	Select the specific country whose current time and date you want the WAP3205 to display.
Finish	Click this to apply the settings and refresh the weather display.

Note: You can also edit the timezone in Section 12.5 on page 107.

6.3 Resetting the WAP3205

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the WAP3205 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.2".

6.3.1 Procedure to Use the Reset Button

1. Make sure the power LED is on.
2. Press the **RESET** button for longer than 1 second to restart/reboot the WAP3205.
3. Press the **RESET** button for longer than five seconds to set the WAP3205 back to its factory-default configurations.

7

Connection Wizard

7.1 Overview

This chapter provides information on the wizard setup screens in the Web Configurator.

The Web Configurator's wizard setup helps you change the system login password and configure your device's operating mode and wireless settings.

7.2 Accessing the Wizard

Launch your web browser and type "http://192.168.1.2" as the website address.

Note: The wizard appears when the WAP3205 is accessed for the first time or when you reset the WAP3205 to its default factory settings.

The wizard screen opens.

Note: If you have already configured the wizard screens and want to open it again, click the **eaZy123** icon on the upper right corner of any Web Configurator screen.

7.2.1 Device Password

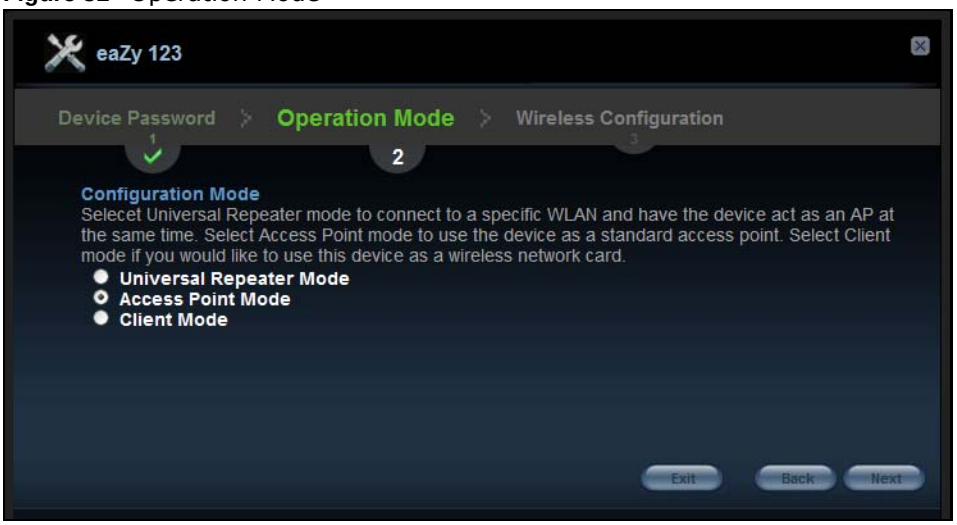
Change the login password in the following screen. Enter the new password and retype it to confirm. Click **Next** to proceed with the **Operation Mode** screen**.**

Figure 30 Device Password

7.2.2 Operation Mode

Select in which device configuration mode you want the WAP3205 to operate. The WAP3205 can act as an access point (AP), wireless client or both at the same time. Click **Next** to configure wireless settings for the selected operation mode.

Figure 31 Operation Mode



7.2.3 Wireless Configuration

Configure the wireless network settings on your WAP3205 in the following screen. The screen varies depending on the device configuration mode.

7.2.3.1 Universal Repeater Mode

When the WAP3205 is in universal repeater mode, the WAP3205 works as an access point and wireless client at the same time. You can let wireless clients connect to another AP or wireless router through the WAP3205 to expand wireless coverage.

Network Selection

Select the wireless device to which you want the WAP3205 to connect and click **Connect**. Click **Refresh** to update the list of available wireless devices.

Figure 32 Wireless Configuration: Select a Network

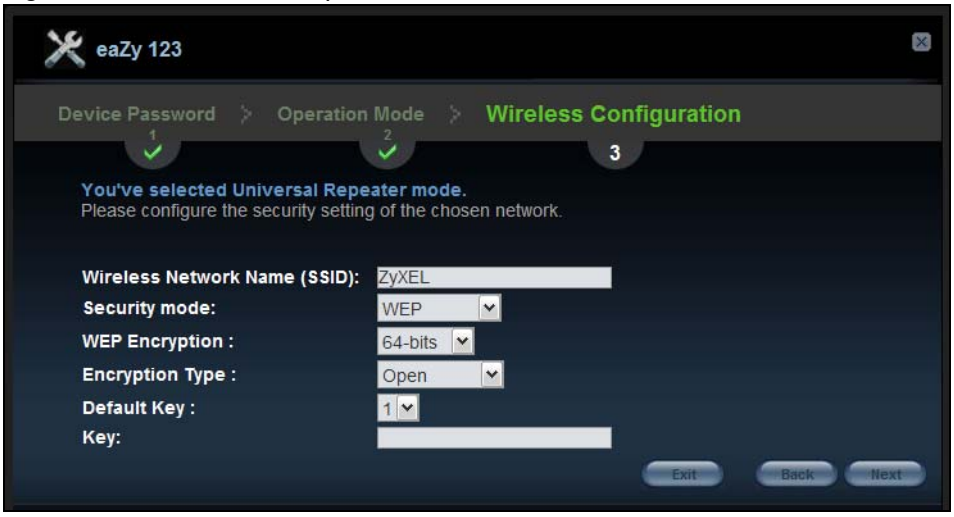
Wireless Security

Configure wireless and wireless security settings. The fields that show up depend on the security type used by the wireless device you selected. The SSID displays automatically. Enter the same security settings as the selected wireless device and click **Next**.

Figure 33 Wireless Security: No Security

Figure 34 Wireless Security: WPA(2)-PSK

Figure 35 Wireless Security: WEP



Settings for Wireless Clients

Select the check box to use the same security settings (as the AP to which the WAP3205 is connecting) for communication between the WAP3205 and its wireless clients. Otherwise, clear the check box and use different SSID and wireless security settings for clients. Click **Next**.

Figure 36 Wireless Configuration: Select a Network

7.2.3.2 Access Point Mode

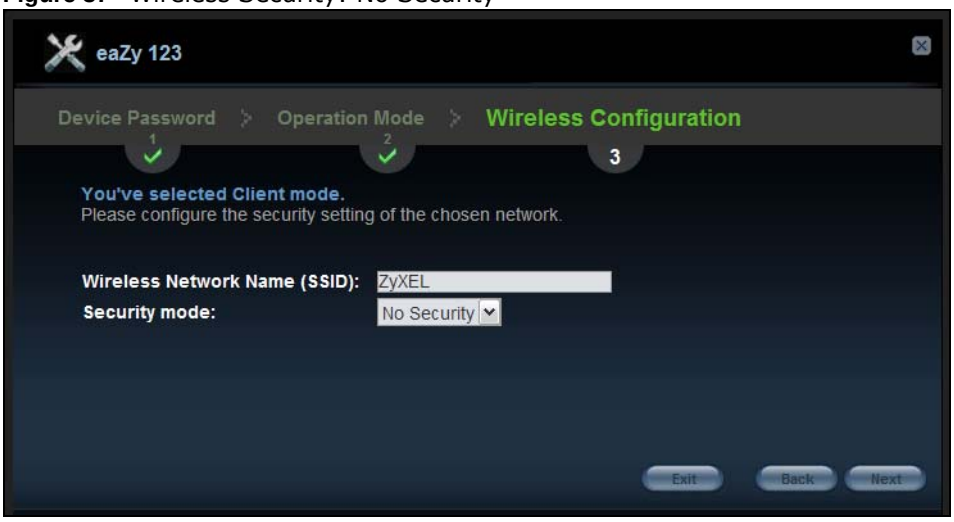
The WAP3205 is in access point mode by default.

Configure wireless and wireless security settings. The fields that show up depend on the kind of security you select.

Wireless Security: No Security

Choose **No Security** in the **Security mode** field to let any wireless device within range access your wireless network.

Figure 37 Wireless Security: No Security



The following table describes the labels in this screen.

Table 23 Wireless Security: No Security

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the WAP3205, make sure all wireless clients use the same SSID in order to access the network.
Security mode	Select a security level from the drop-down list box. Choose **None** to have no wireless LAN security configured. If you do not enable any wireless security on your WAP3205, your network is accessible to any wireless networking device that is within range.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

Wireless Security: WPA-PSK/WPA2-PSK

Choose **WPA-PSK** or **WPA2-PSK** security in the **Security mode** field to set up a password for your wireless network.

Figure 38 Wireless Security: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 24 Wireless Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the WAP3205, make sure all wireless stations use the same SSID in order to access the network.
Security mode	Choose **WPA-PSK** or **WPA2-PSK** security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively.
Wireless password	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens.

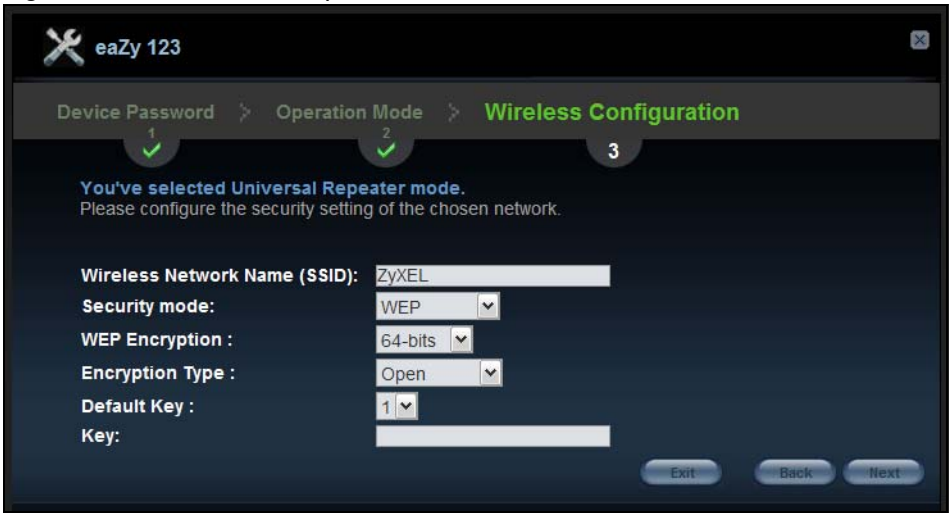
Table 24 Wireless Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Verify Password	Retype the password to confirm.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

Wireless Security: WEP

Choose **WEP** security in the **Security mode** field to configure a WEP key for your wireless network.

Figure 39 Wireless Security: WEP



The following table describes the labels in this screen.

Table 25 Wireless Security: WEP

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the WAP3205, make sure all wireless stations use the same SSID in order to access the network.
Security mode	Choose **WEP** security to enable data encryption using WEP keys.
WEP Encryption	Select **64-bits** or **128-bits**. This dictates the length of the security key that the network is going to use.
Authentication Method	Select **Open** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Select **Shared Key** to force the clients to provide the WEP key prior to communication. Otherwise, select **Open**.
Default Key	You can configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time. Select a default WEP key to use for data encryption.

Table 25 Wireless Security: WEP

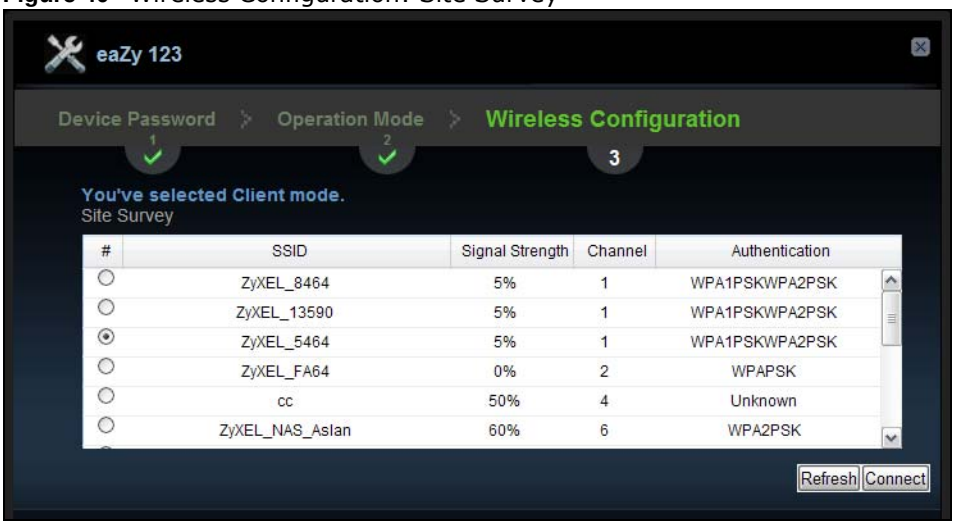
LABEL	DESCRIPTION
Key	If you chose **64-bit**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

7.2.3.3 Client Mode

In this mode, the WAP3205 is a wireless client. Clients can access the WAP3205 through a wired connection only.

Select the wireless device to which you want the WAP3205 to connect and click **Connect**. Click **Refresh** to update the list of available wireless devices.

Figure 40 Wireless Configuration: Site Survey



Wireless Security

Configure wireless and wireless security settings. The fields that show up depend on the security type used by the wireless device you selected. The SSID displays automatically. Enter the same security settings as the selected wireless device and click **Next**.

Figure 41 Wireless Security: No Security

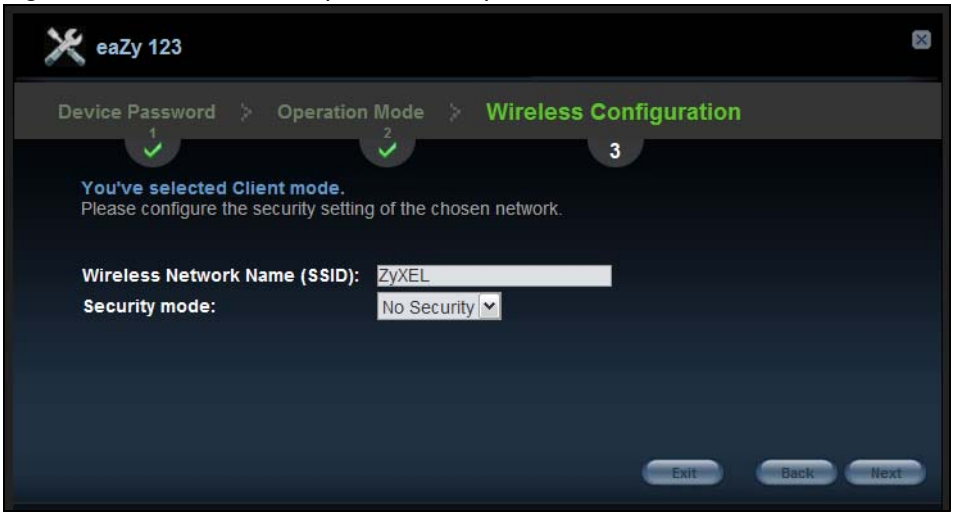


Figure 42 Wireless Security: WPA(2)-PSK

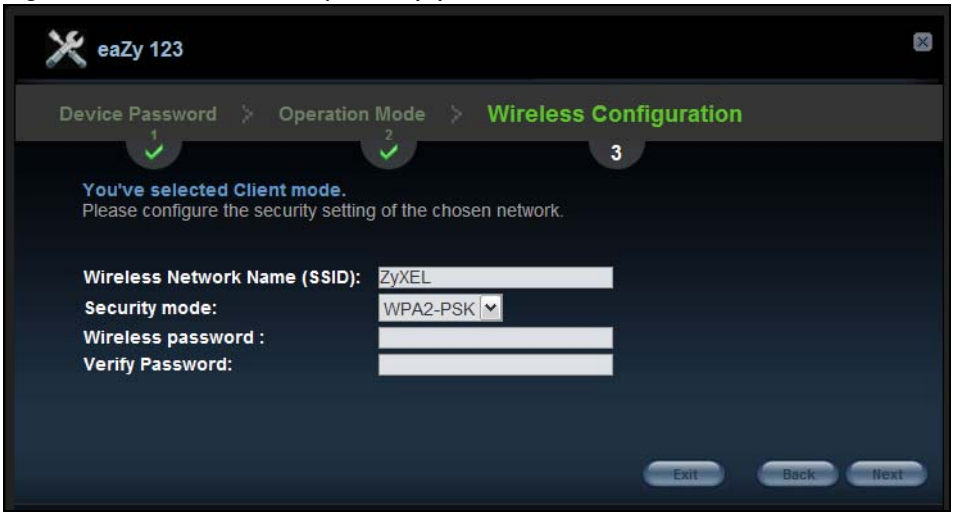
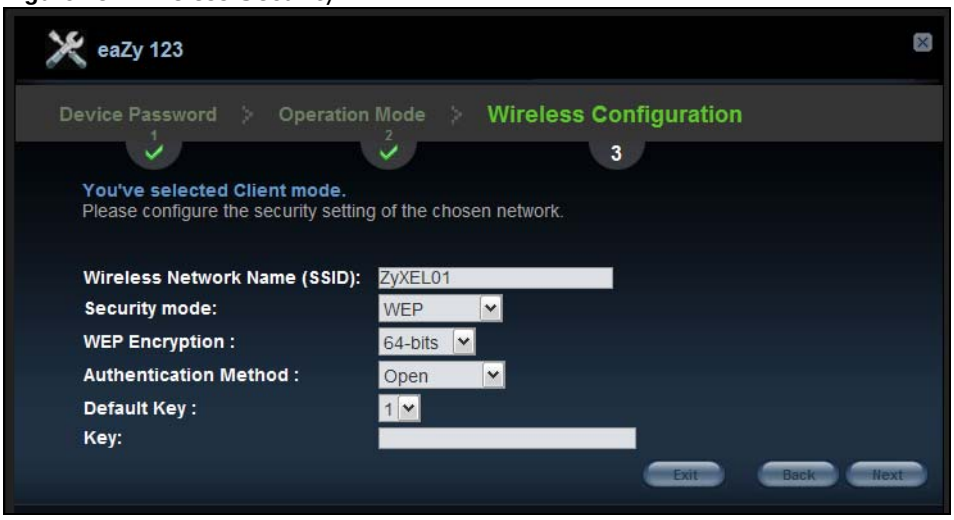


Figure 43 Wireless Security: WEP



7.2.3.4 Wizard Setup Complete

Click **GO** to reboot the WAP3205 and finish wizard configuration.

Figure 44 Wizard Setup Complete

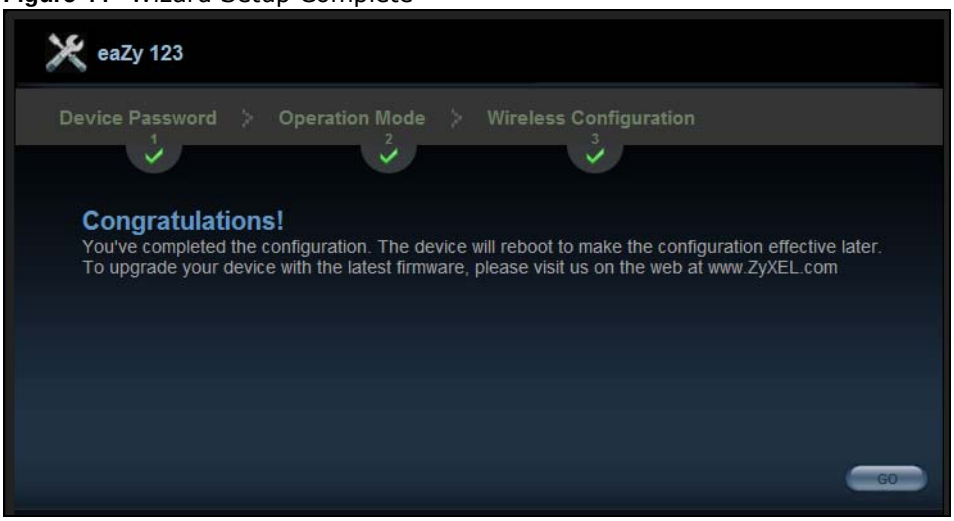
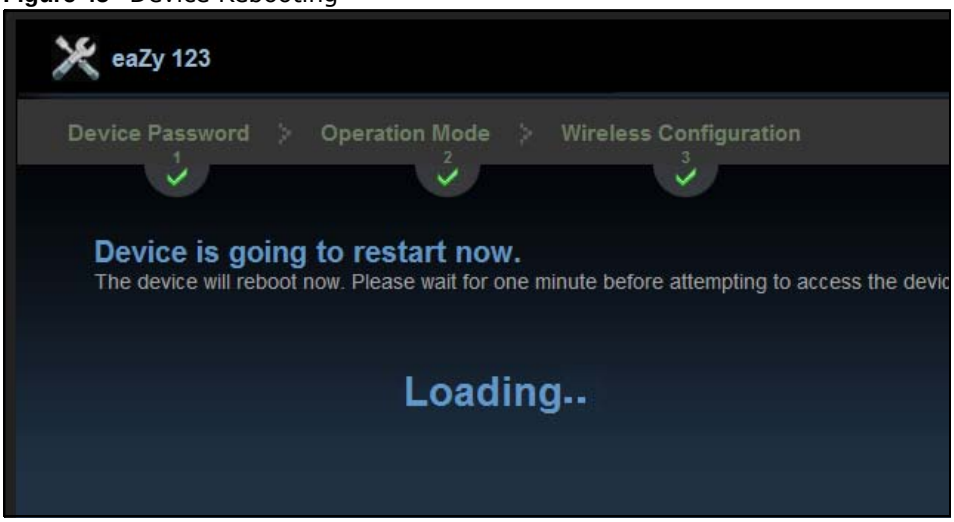


Figure 45 Device Rebooting



Congratulations! After the WAP3205 restarts, the login screen displays. You have successfully set up your WAP3205 to operate on your network and access the Internet. You are now ready to connect wirelessly to your WAP3205 and access the Internet.

You can access the Web Configurator of your WAP3205 for advanced settings, or open a web browser, such as Internet Explorer, to visit your favorite website.

8

Tutorials

8.1 Overview

This chapter provides tutorials for your WAP3205 (in access point or universal repeater mode) as follows:

- Connecting to the Internet from an Access Point
- Configuring Wireless Security Using WPS
- Enabling and Configuring Wireless Security (No WPS)
- Using Multiple SSIDs on the WAP3205
- Connecting the WAP3205 (in Universal Repeater Mode) to an AP or Wireless Router

This chapter provides tutorials for your WAP3205 (in client mode) as follows:

- Connecting the WAP3205 (in Client Mode) to an AP or Wireless Router

8.2 Connecting to the Internet from an Access Point

This section gives you an example of how to set up an access point (AP) and wireless client (a notebook (**B**), in this example) for wireless communication. **B** can access the Internet through the access point (**A**) wirelessly.

Figure 46 Wireless Access Point Connection to the Internet

8.3 Configuring Wireless Security Using WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the WAP3205 as the AP and NWD-211AN as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 8.3.1 on page 60.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the WAP3205's interface. See Section 8.3.2 on page 61. This is the more secure method, since one device can authenticate the other.

8.3.1 Push Button Configuration (PBC)

1. Make sure that your WAP3205 is turned on and that it is within range of your computer.
2. Make sure that you have installed the wireless client (this example uses the NWD-211AN) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
4. Log into WAP3205's Web Configurator and press the **Push Button** button in the **Network** > **Wireless Client** > **WPS Station** screen.

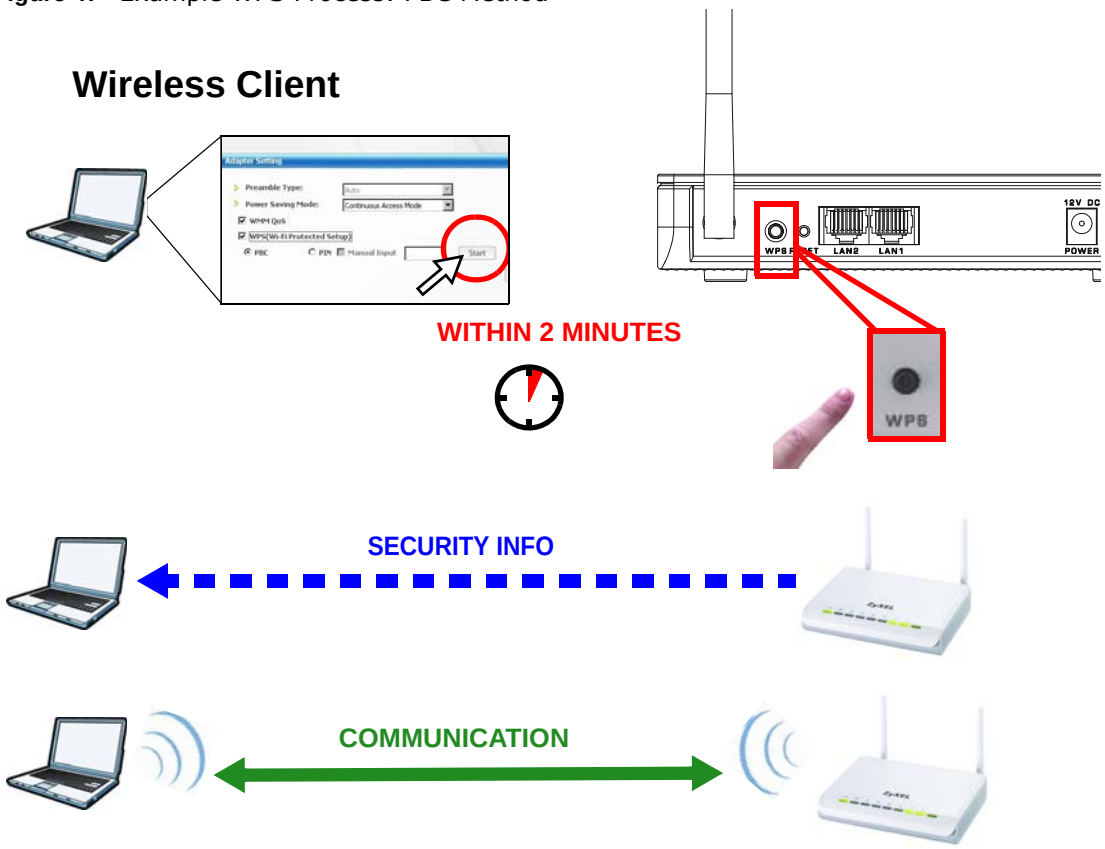
   Note: Your WAP3205 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

   Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

   The WAP3205 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WAP3205 securely.

   The following figure shows you how to set up wireless network and security by pressing a button on both WAP3205 and wireless client (the NWD-211AN in this example).

Figure 47 Example WPS Process: PBC Method



8.3.2 PIN Configuration

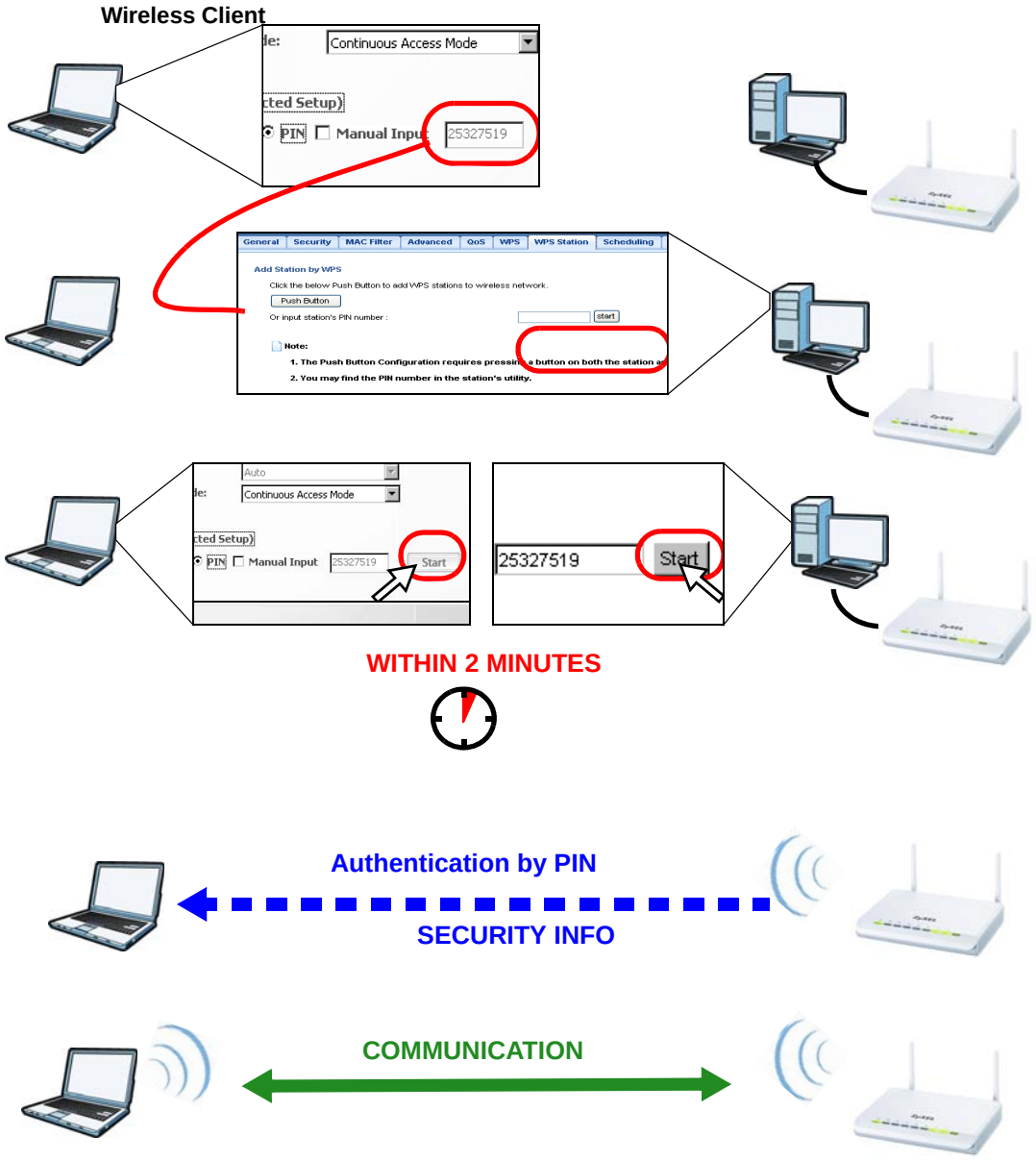
When you use the PIN configuration method, you need to use both WAP3205's configuration interface and the client's utilities.

1. Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
2. Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the WAP3205.
3. Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the WAP3205's **WPS Station** screen within two minutes.

   The WAP3205 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WAP3205 securely.

   The following figure shows you how to set up wireless network and security on WAP3205 and wireless client (NWD-211AN in this example) by using PIN method.

Figure 48 Example WPS Process: PIN Method



8.4 Enabling and Configuring Wireless Security (No WPS)

This example shows you how to configure wireless security settings with the following parameters on your WAP3205.

SSID	SSID_Example3

Channel	Auto
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

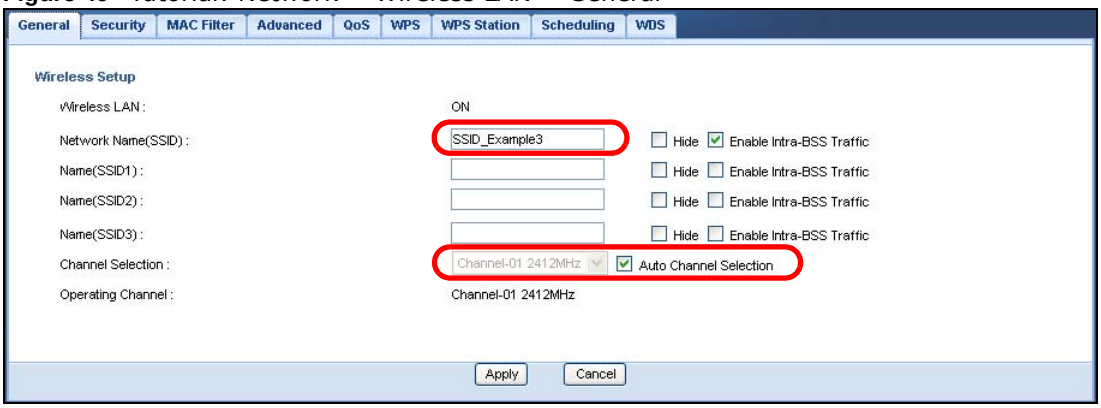
Follow the steps below to configure the wireless settings on your WAP3205.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 6.2 on page 43).

1 Open the **Wireless LAN > General** screen in the AP's Web Configurator.

2 Enter **SSID_Example3** as the SSID and select a channel or select **Auto Channel Selection** to have the WAP3205 scans for and select an available channel automatically. Click **Apply**.

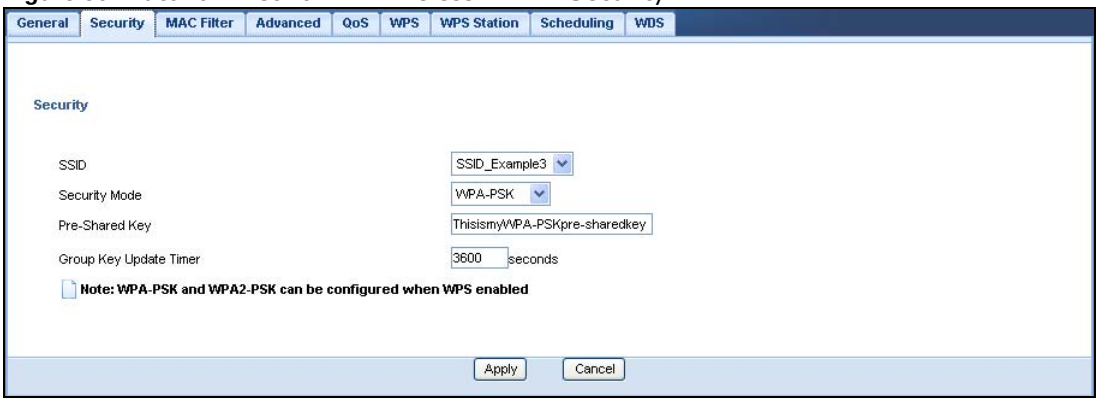
Figure 49 Tutorial: Network > Wireless LAN > General



3 Click the **Security** tab.

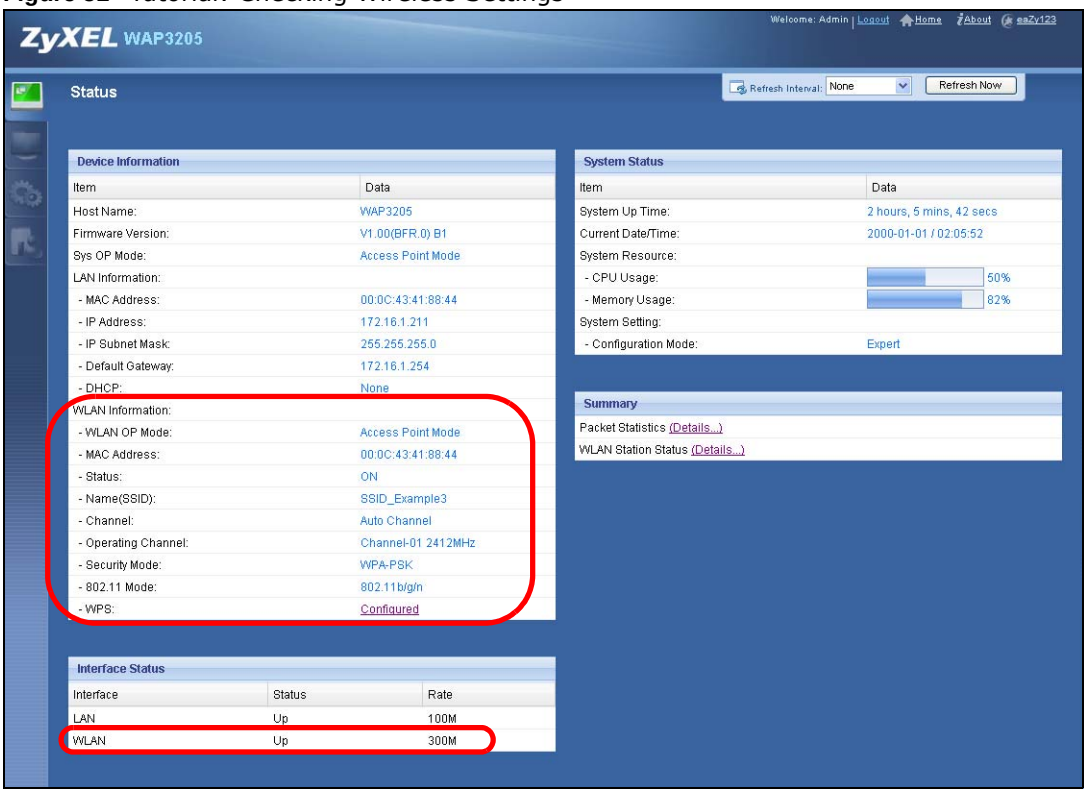
4 Select the SSID (**SSID_Example3**) for which you want to configure the security. Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 50 Tutorial: Network > Wireless LAN > Security



5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 51 Tutorial: Checking Wireless Settings



8.4.1 Configure Your Notebook

Note: We use the ZyXEL NWD-211AN wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

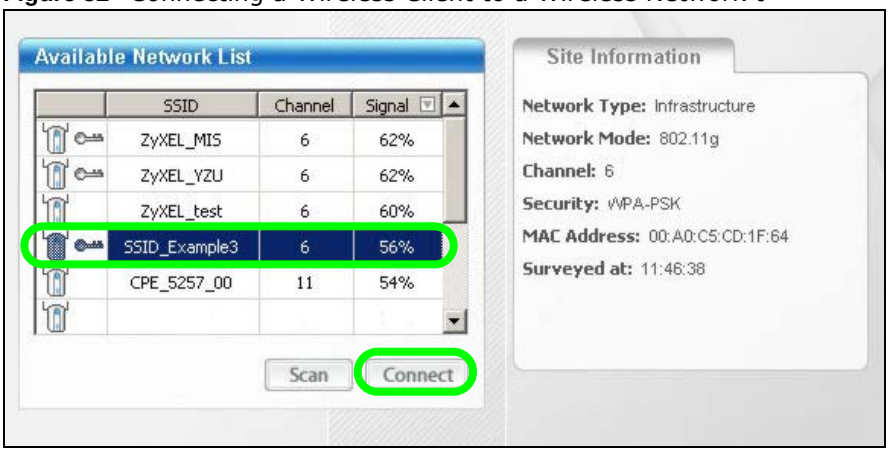
1 The WAP3205 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

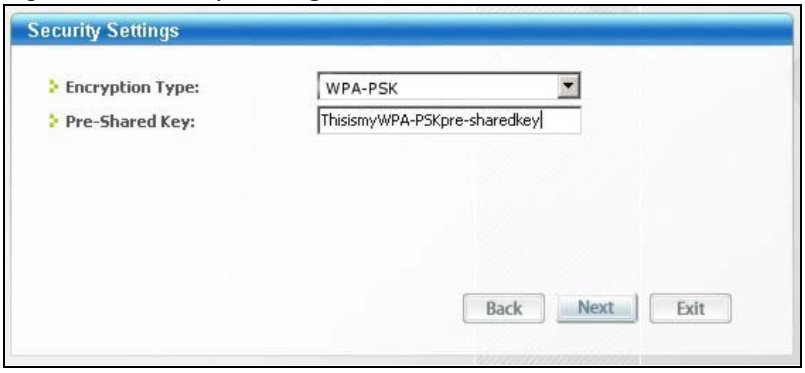
4 Select SSID_Example3 and click **Connect**.

Figure 52 Connecting a Wireless Client to a Wireless Network t



5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 53 Security Settings

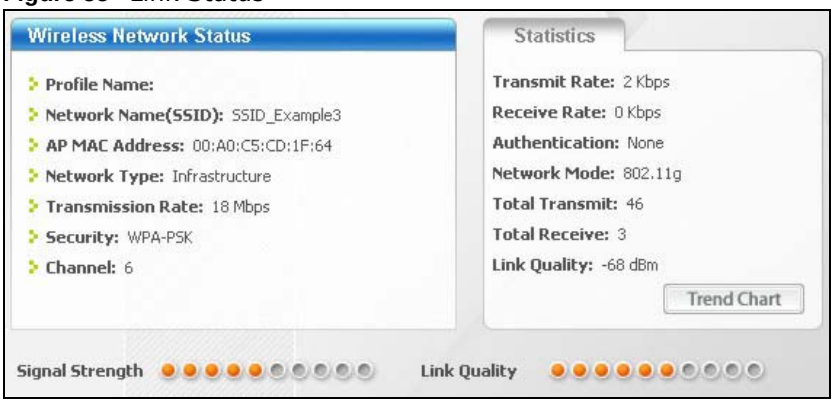


6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 54 Confirm Save

7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 55 Link Status



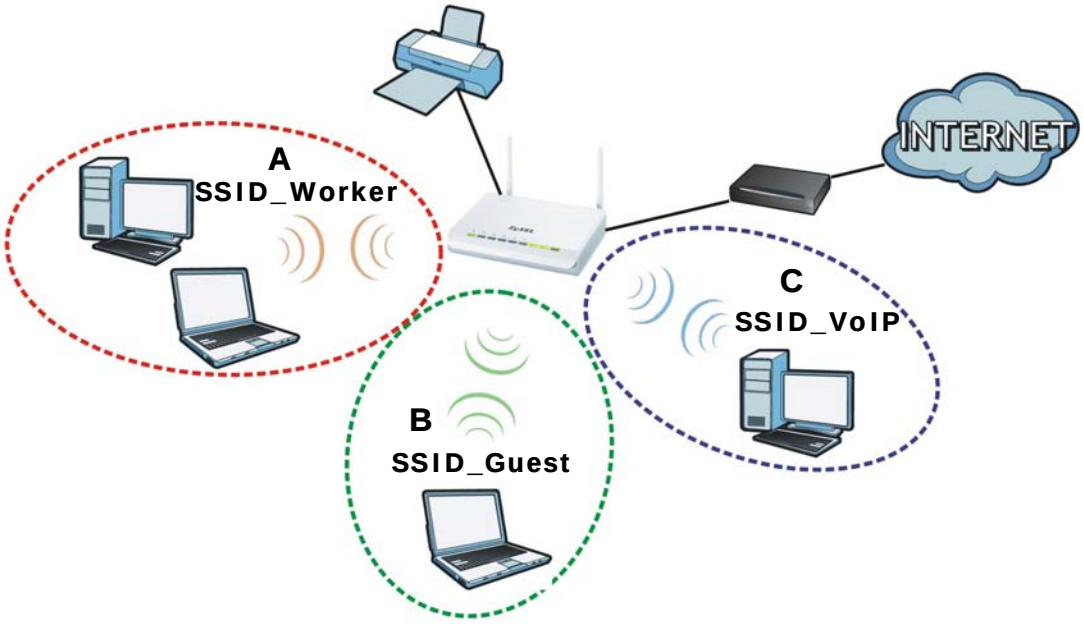
If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

8.5 Using Multiple SSIDs on the WAP3205

You can configure more than one SSID on a WAP3205 when it is operating in access point or universal repeater mode. This allows you to configure multiple independent wireless networks on the WAP3205 as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, wireless security type and MAC filtering settings. That is, each SSID on the WAP3205 represents a different access point/wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the WAP3205 (such as a printer), but they cannot listen to each other's traffic.

For example, you may set up three wireless networks (**A**, **B** and **C**) in your office. **A** is for workers, **B** is for guests and **C** is specific to a VoIP device in the meeting room.



8.5.1 Configuring Security Settings of Multiple SSIDs

The WAP3205 is in access point mode by default. If you want to use multiple SSIDs when the WAP3205 is in universal repeater mode, see Chapter 5 on page 35 for how to set the WAP3205 to universal repeater mode.

This example shows you how to configure the SSIDs with the following parameters on your WAP3205 (in access point mode).

SSID	SECURITY TYPE	KEY	MAC FILTERING
SSID_Worker	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork	Disable
SSID_Guest	Static WEP 128bit	keyexample123	Disable
SSID_VoIP	WPA-PSK	VoIPOnly12345678	Allow 00:A0:C5:01:23:45

1 Connect your computer to the LAN port of the WAP3205 using an Ethernet cable.

2 The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

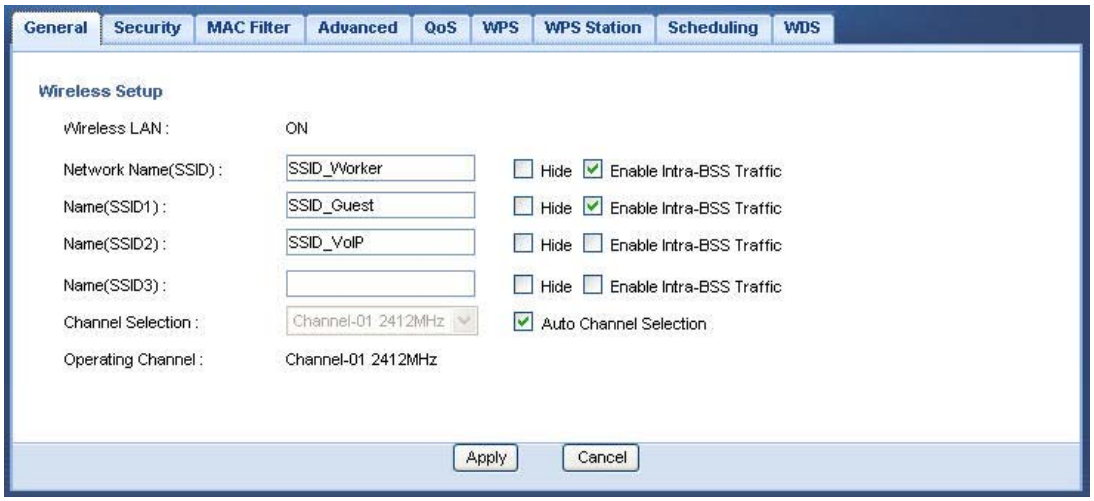
3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 141 for information on changing your computer's IP address.

4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

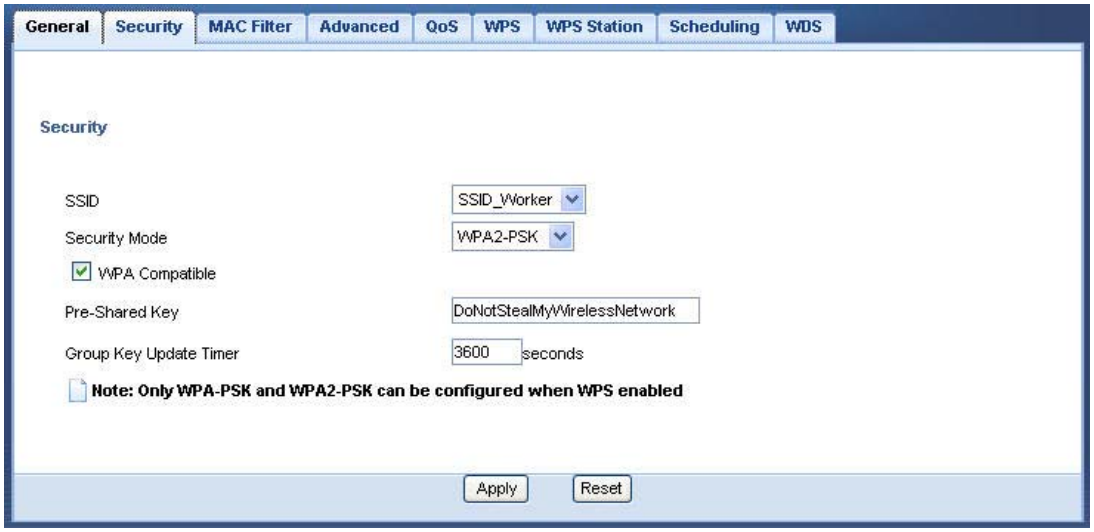
5 Enter "1234" (default) as the password and click **Login**.

6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

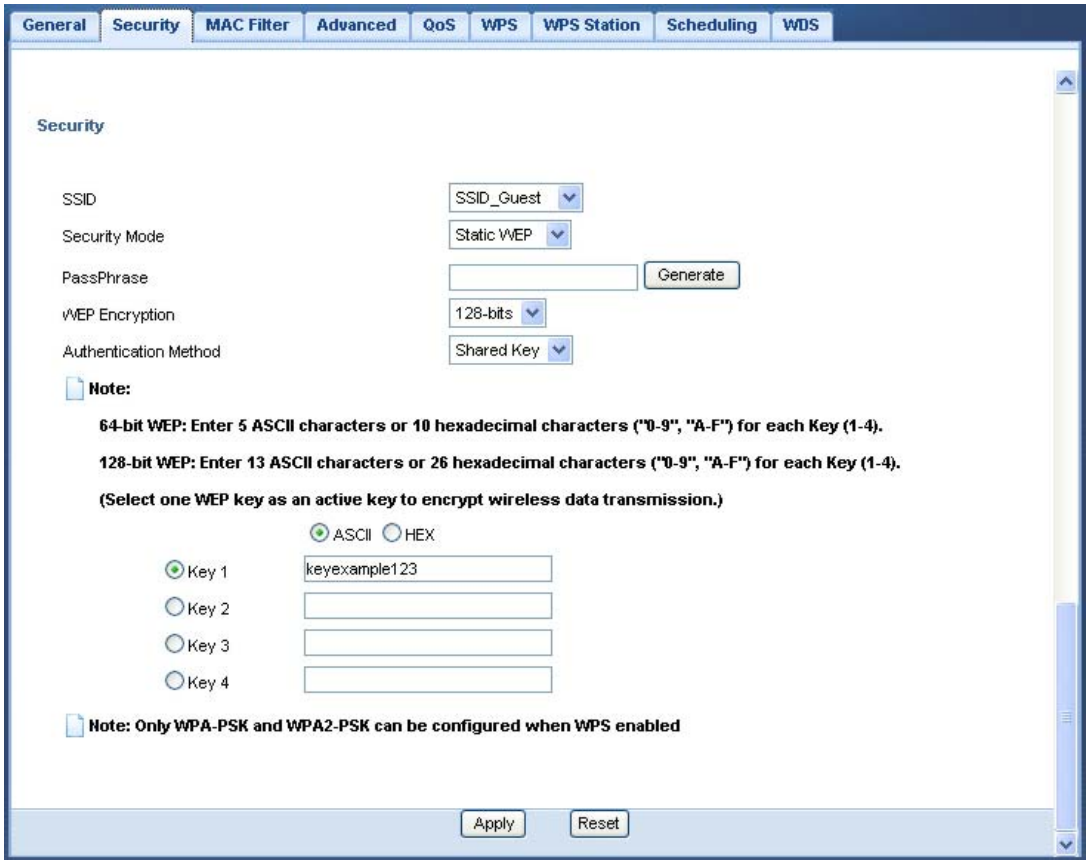
7 Go to **Configuration > Network > Wireless LAN > General**. Configure the screen as follows. In this example, you select **Enable Intra-BSS Traffic** for SSID_Worker and SSID_Guest to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.



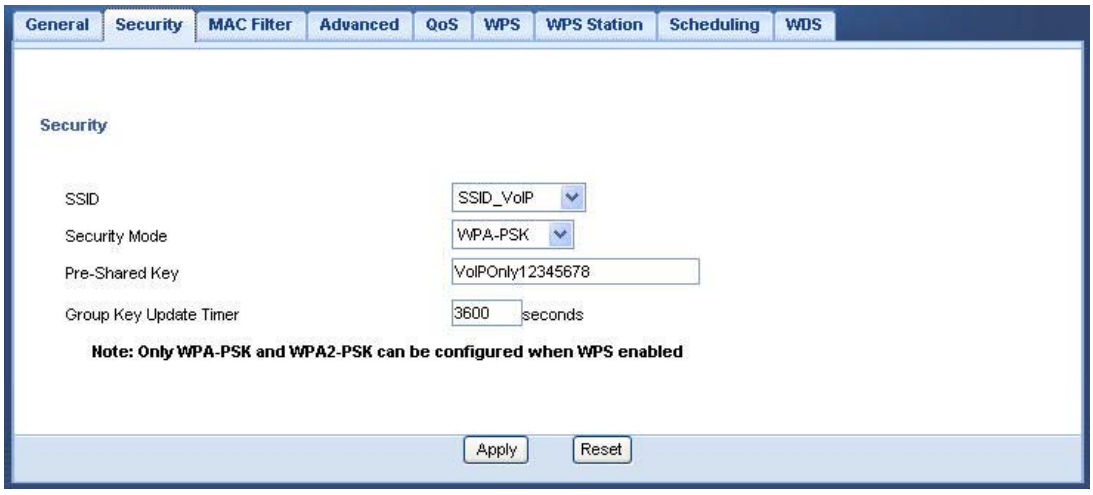
8 Click the **Security** tab to configure security settings for each SSID. Select **SSID_Worker** from the **SSID** drop-down list. Configure the screen as follows. Click **Apply**.



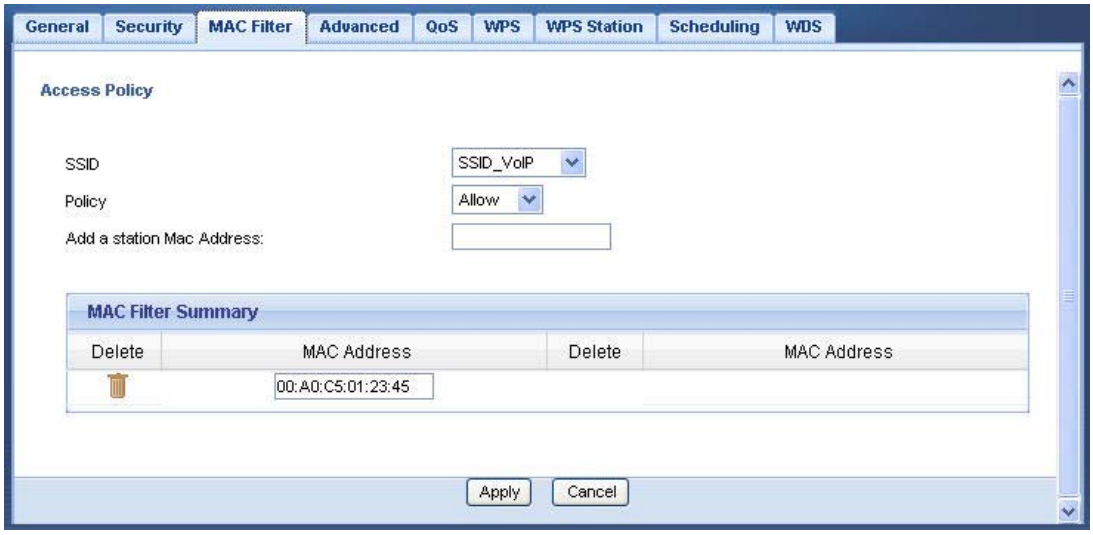
9 Select **SSID_Guest** from the **SSID** drop-down list. Configure the screen as follows. Click **Apply**.



10 Select **SSID_VoIP** from the **SSID** drop-down list. Configure the screen as follows. Click **Apply**.



11 Click the **MAC Filter** tab to configure MAC filtering for the **SSID_VoIP** wireless network. Select **SSID_VoIP** from the **SSID** drop-down list and select **Allow** in the **Policy** field. Enter the VoIP device's MAC address in the **Add a station Mac Address** field and click **Apply** to allow only the VoIP device to associate with the WAP3205 using this SSID.



8.6 Connecting the WAP3205 (in Universal Repeater Mode) to an AP or Wireless Router

If you have an access point or wireless router with Internet access deployed in your network already, and you want to have wireless clients connect to the existing AP or wireless router through the WAP3205, set the WAP3205 to universal repeater mode and then associate the WAP3205 with the AP or wireless router. The WAP3205 must be within the transmission range of the AP or wireless router.

1 Connect your computer to the LAN port of the WAP3205 using an Ethernet cable.

2 The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 141 for information on changing your computer's IP address.

4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

5 Enter "1234" (default) as the password and click **Login**.

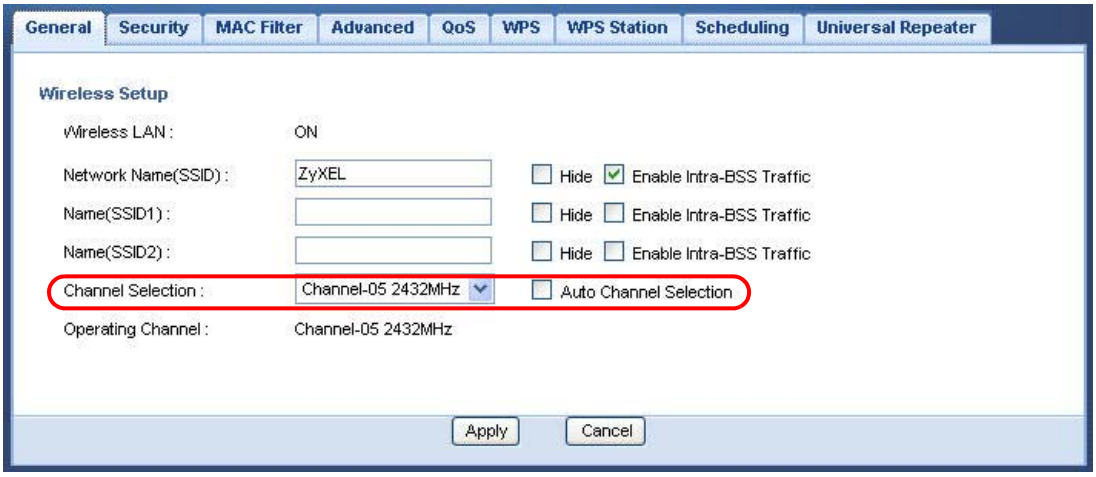
6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

7 On the left of the screen, click **Maintenance > Sys OP Mode** and select **Universal Repeater Mode**. Click **Apply**. The WAP3205 restarts.

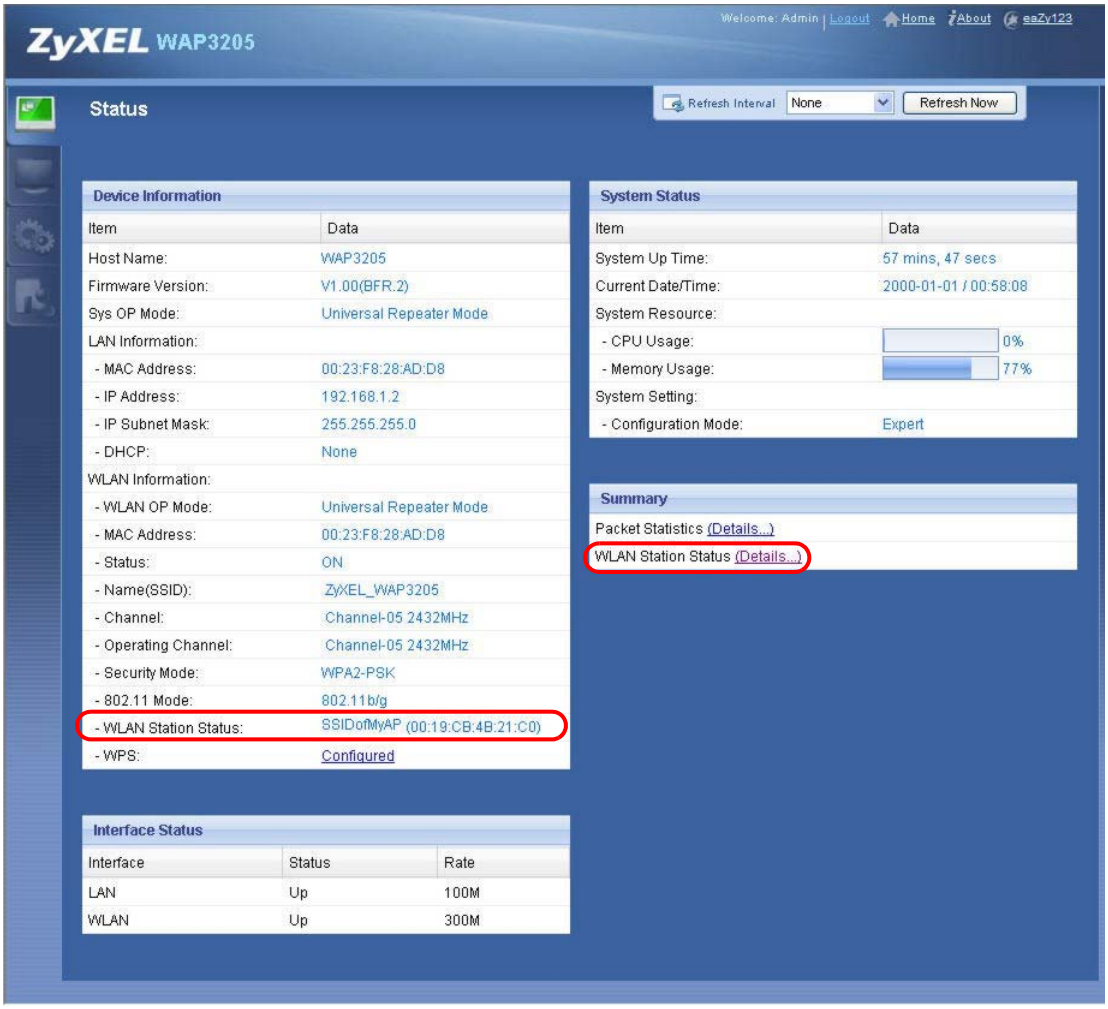
8 Enter the password and click **Login** to access the web configurator again.

9 Go to **Configuration > Network > Wireless LAN > Universal Repeater** to connect the WAP3205 wirelessly to an AP. Select **Enable**. Enter the SSID of the existing AP or wireless router to which you want to connect ("SSIDofMyAP" in this example). Enter the wireless security settings which are the same as those on the existing AP or wireless router to access it (WPA-PSK and "KeyofMyWirelessNetwork" in this example). Click **Apply**.

10 Set the channel number in the **Wireless LAN > General** screen to be the same as the one on the wireless router or AP to which the WAP3205 is connecting. This allows wireless clients access or acquire an IP address from another AP or wireless router through the WAP3205 in universal repeater mode.



11 Go to the **Status** screen. If the WAP3205 has successfully connected to an AP or wireless router, it displays the SSID and MAC address of the AP or wireless router in the field next to **WLAN Station Status** under **Device Information**.



To check whether a wireless client is currently connecting to the WAP3205, click the **WLAN Station Status (Details...)** hyperlink under **Summary** in the **Status** screen or **Monitor > WLAN Station Status**. See Section 9.5 on page 83 for more information.

8.7 Connecting the WAP3205 (in Client Mode) to an AP or Wireless Router

If you have an access point or wireless router with Internet access deployed in your network already, and you want to use the WAP3205 as a wireless client to connect to the existing AP or wireless router, set the WAP3205 to client mode. The WAP3205 then acts as a wireless client. Your device, such as a computer, can connect to the WAP3205 through a wired connection to access the Internet.

1 Connect your computer to the LAN port of the WAP3205 using an Ethernet cable.

2 The default IP address of the WAP3205 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

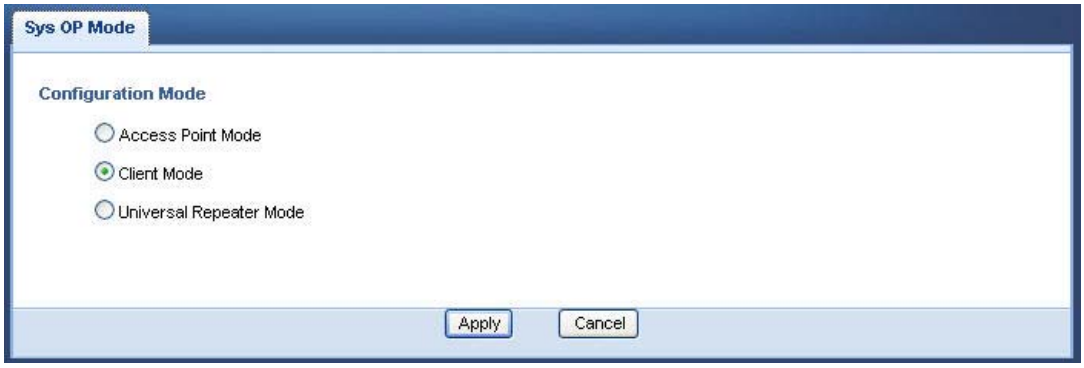
3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 141 for information on changing your computer's IP address.

4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

5 Enter "1234" (default) as the password and click **Login**.

6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

7 On the left of the screen, click **Maintenance > Sys OP Mode** and select **Client Mode**. Click **Apply**. The WAP3205 restarts.

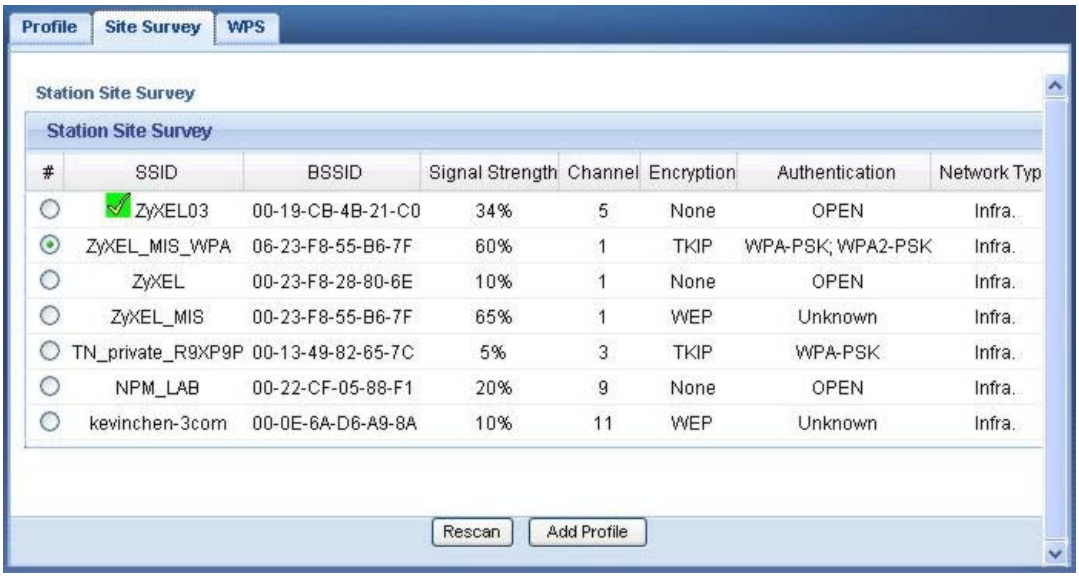


8 Enter the password and click **Login** to access the web configurator again.

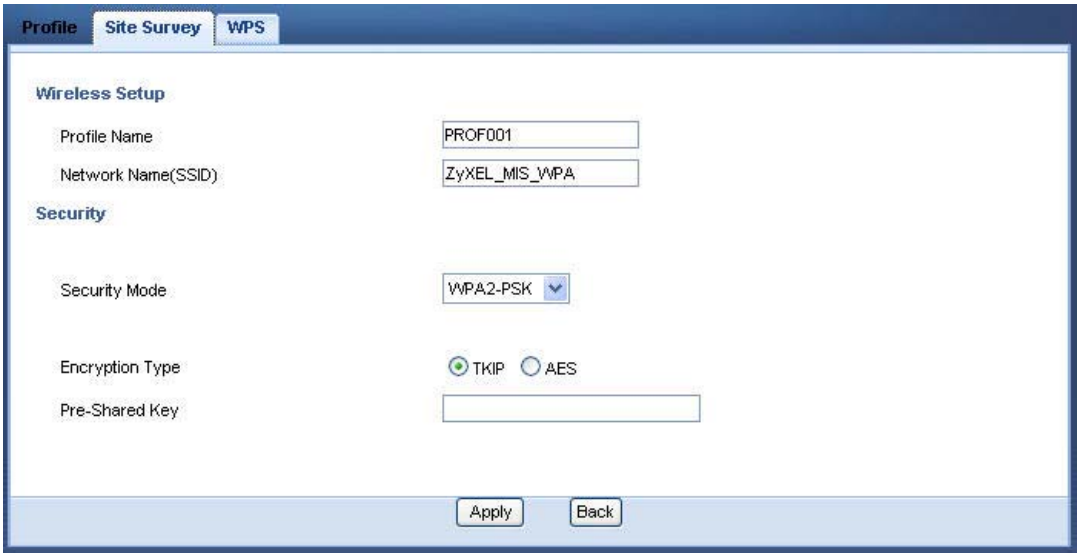
9 To connect to a specific wireless network, you can manually create a wireless profile or use the site survey tool to associate with it.

8.7.1 Connecting to a Wireless Network Using Site Survey

1 Go to **Configuration > Network > Wireless LAN > Site Survey**. The WAP3205 automatically scans for and connects to an available wireless network. The green check icon indicates the wireless device to which the WAP3205 is connecting. Select an SSID's radio button and click **Add Profile** to add this wireless device to a profile.



2 Enter a new profile name or use the name generated automatically by the system. Enter the security settings if requested and click **Apply**. The security settings must be the same as those on the AP to which you are connecting.

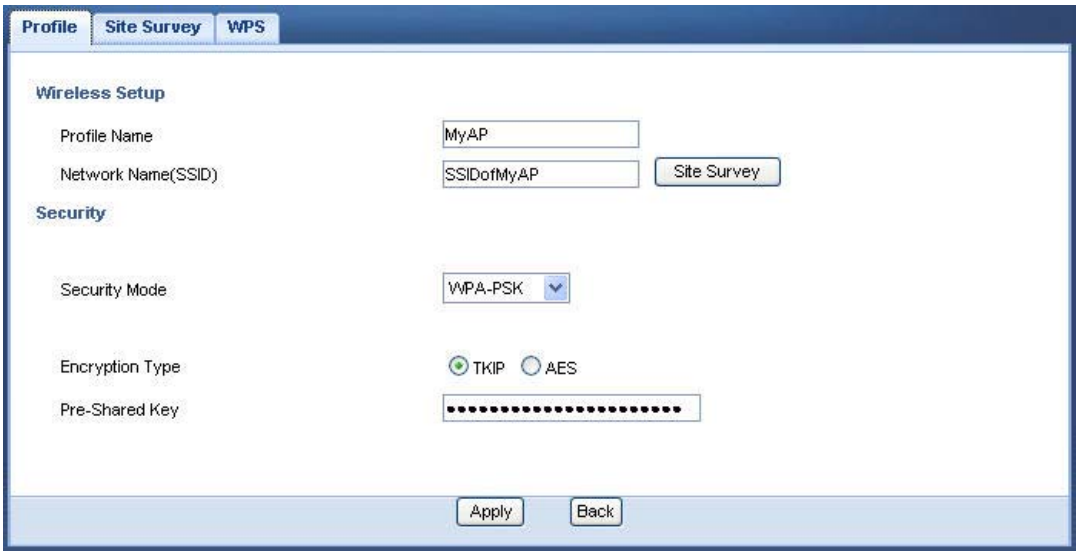


3 The new profile entry displays in the Profile screen. The green check icon means this profile is active and the WAP3205 is associating with the specified wireless network.

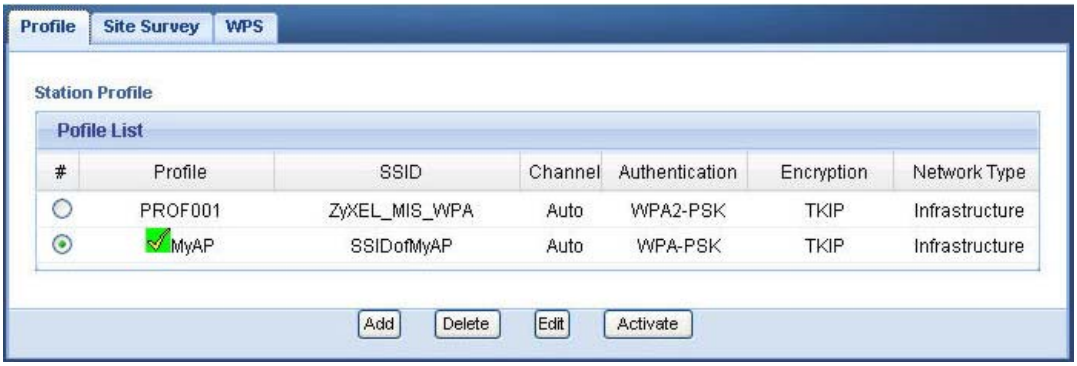
8.7.2 Connecting to a Wireless Network Using a Profile

1 Go to **Configuration > Network > Wireless LAN > Profile**. Click **Add** to manually create a wireless LAN profile.

2 Enter a descriptive profile name and the SSID and security settings of the wireless device to which you want to connect. Click **Apply**.



3 The new profile entry displays in the **Profile** screen. To enable a profile, select the corresponding radio button and click **Activate**. The green check icon means this profile is active and the WAP3205 is associating with the specified wireless network.



8.7.3 Deploying the WAP3205 in your Network

1. After you finish configuring the operating mode and wireless settings on the WAP3205, disconnect the computer from the WAP3205 and change its TCP/IP settings back to the previous ones.

2. Connect a device to the WAP3205, which you want to use to access the AP or wireless router through the WAP3205. Make sure the device is set to obtain an IP address automatically.

PART II
Technical Reference

9

Monitor

9.1 Overview

This chapter discusses read-only information related to the device state of the WAP3205.

Note: To access the Monitor screens, you can also click the links in the Summary table of the Status screen to view the packets sent/received as well as the status of clients connected to the WAP3205.

9.2 What You Can Do

- Use the **Log** screen (Section 9.3 on page 81) to view the logs for the categories such as system maintenance, system errors, and so on.
- use the **Packet Statistics** screen (Section 9.4 on page 82) to view port status, packet specific statistics, the "system up time" and so on.
- Use the **WLAN Station Status** screen (Section 9.5 on page 83) to view the wireless stations that are currently associated to the WAP3205.

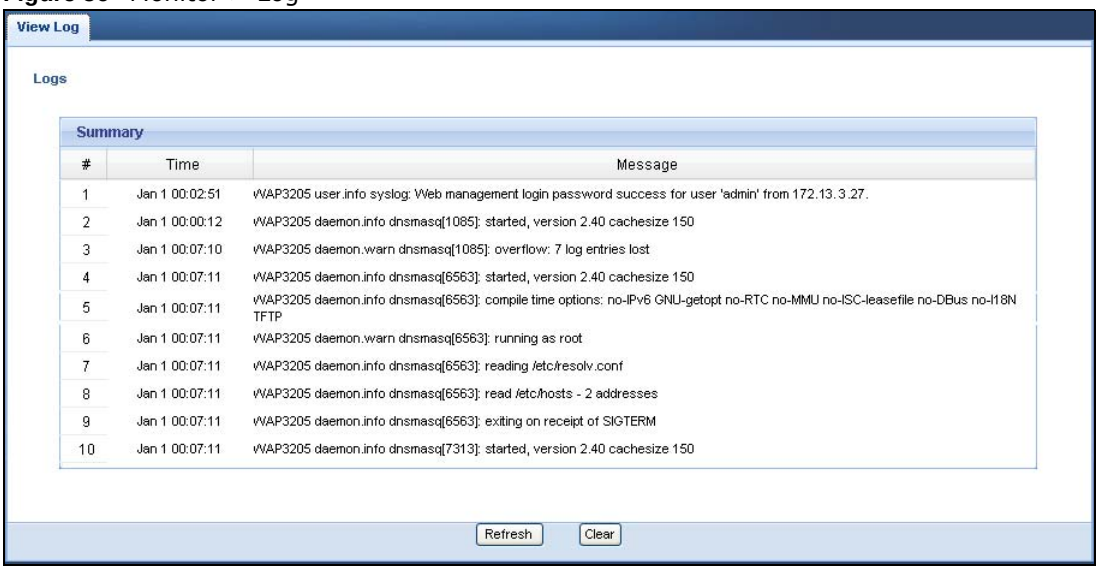
9.3 Log

Use the **View Log** screen to see the logged messages for the WAP3205.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills.

Click **Monitor** > **Log**.

Figure 56 Monitor > Log



The following table describes the labels in this screen.

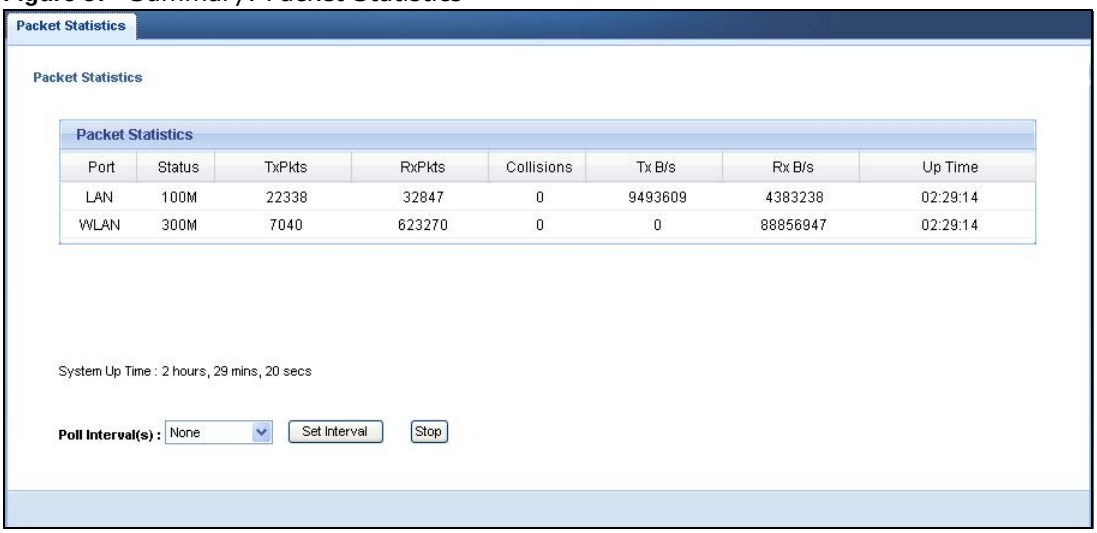
Table 26 Monitor > Log

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Refresh	Click **Refresh** to renew the log screen.
Clear	Click **Clear** to delete all the logs.

9.4 Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen or **Monitor** > **Packet Statistics**. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 57 Summary: Packet Statistics



The following table describes the labels in this screen.

Table 27 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the WAP3205's port type.
Status	For the LAN ports, this displays the port speed or **Down** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the WAP3205 has been for each session.
System Up Time	This is the total time the WAP3205 has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

9.5 WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen or **Monitor** > **WLAN Station Status**. View the wireless stations that are currently associated to the WAP3205 in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Note: This screen is not available when the WAP3205 is in Client mode.

Figure 58 Summary: Wireless Association List

The following table describes the labels in this screen.

Table 28 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the WAP3205's WLAN network.
Refresh	Click **Refresh** to reload the list.

10

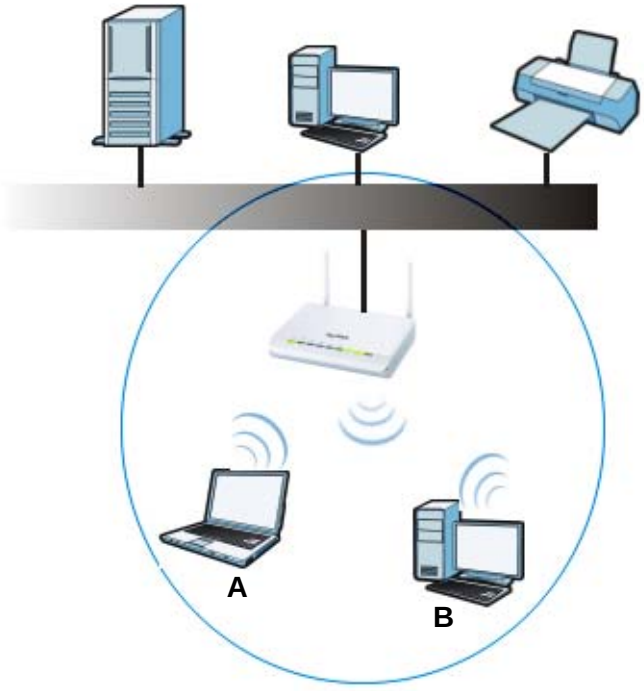
Wireless LAN

10.1 Overview

This chapter discusses how to configure the wireless network settings in your WAP3205. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 59 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your WAP3205 is the AP.

10.2 What You Can Do

- Use the **General** screen (Section 10.4 on page 88) to enter the SSID, enable intra-BSS traffic and select the channel.
- Use the **Security** screen (Section 10.5 on page 89) to configure wireless security between the WAP3205 and the wireless clients.

- Use the **MAC Filter** screen (Section 10.6 on page 93) to allow or deny wireless stations based on their MAC addresses from connecting to the WAP3205.
- Use the **Advanced** screen (Section 10.7 on page 94) to configure wireless advanced features, such as set the RTS/CTS Threshold and HT physical mode.
- Use the **QoS** screen (Section 10.8 on page 95) to enable Wifi MultiMedia Quality of Service (WMMQoS). This allows the WAP3205 to automatically set priority levels to services, such as e-mail, VoIP, chat, and so on.
- Use the **WPS** screen (Section 10.9 on page 96) to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen (Section 10.10 on page 97) to add a wireless station using WPS.
- Use the **Scheduling** screen (Section 10.11 on page 97) to set the times your wireless LAN is turned on and off.
- Use the **WDS** screen (Section 10.12 on page 98) to configure Wireless Distribution System on your WAP3205.

10.3 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

10.3.1 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

10.3.1.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

10.3.1.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or

00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

10.3.1.3 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication.

Table 29 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION
Weakest	No Security
↕	WEP
	WPA-PSK
Strongest	WPA2-PSK

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA-PSK. Therefore, you should set up **WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK** or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

When you select **WPA2-PSK** in your WAP3205, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** (depending on the type of wireless network login) and select the **WPA Compatible** option in the WAP3205.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

10.3.1.4 WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 8.3 on page 59.

10.3.1.5 WDS

Wireless Distribution System or WDS security is used between bridged APs. It is independent of the security between the wired networks and their respective APs. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key.

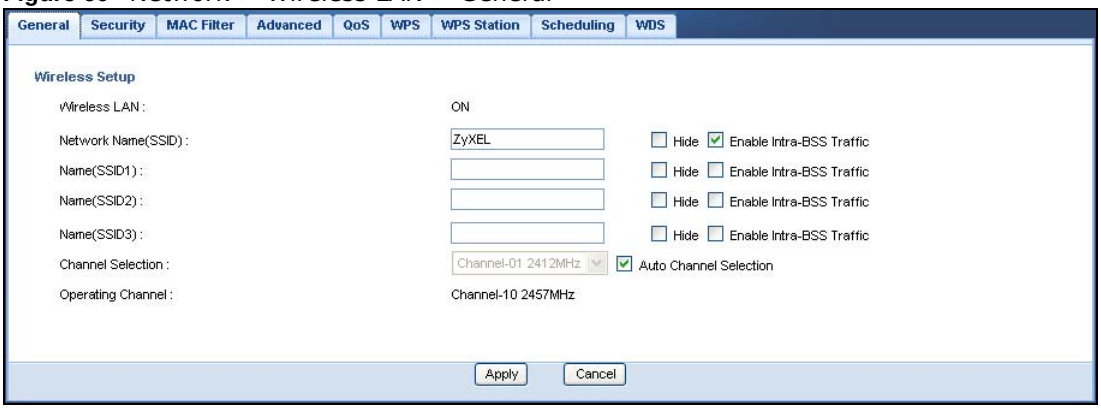
10.4 General Wireless LAN Screen

Use this screen to enter the SSID, select the channel and enable intra-BSS traffic.

Note: If you are configuring the WAP3205 from a computer connected to the wireless LAN and you change the WAP3205's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the WAP3205's new settings.

Click **Network** > **Wireless LAN** to open the **General** screen.

Figure 60 Network > Wireless LAN > General



The following table describes the general wireless LAN labels in this screen.

Table 30 Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN	This is turned on by default. The current wireless state is reflected in this field.

Table 30 Network > Wireless LAN > General

LABEL	DESCRIPTION
Network Name(SSID) or Name(SSID1~3)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN. You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the WAP3205. This allows you to use one access point to provide several BSSs simutaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a wireless client cannot obtain the SSID through scanning using a site survey tool.
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. This option is only available if **Auto Channel Selection** is disabled.
Auto Channel Selection	Select the check box to have the WAP3205 automatically scan for and select a channel which is not used by another device.
Operating Channel	This displays the channel the WAP3205 is currently using.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.5 Wireless Security Screen

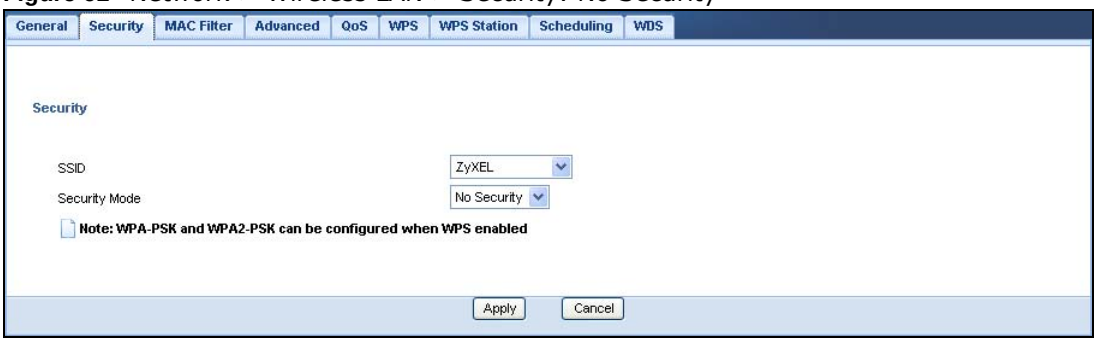
Use this screen to select the wireless security mode for each SSID. Click **Network** > **Wireless LAN** > **Security** to open the **Security** screen. The screen varies depending on what you select in the **Security Mode** field.

10.5.1 No Security

Select **No Security** to allow wireless clients to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your WAP3205, your network is accessible to any wireless networking device that is within range.

Figure 61 Network > Wireless LAN > Security: No Security



The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > Security: No Security

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure the security.
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

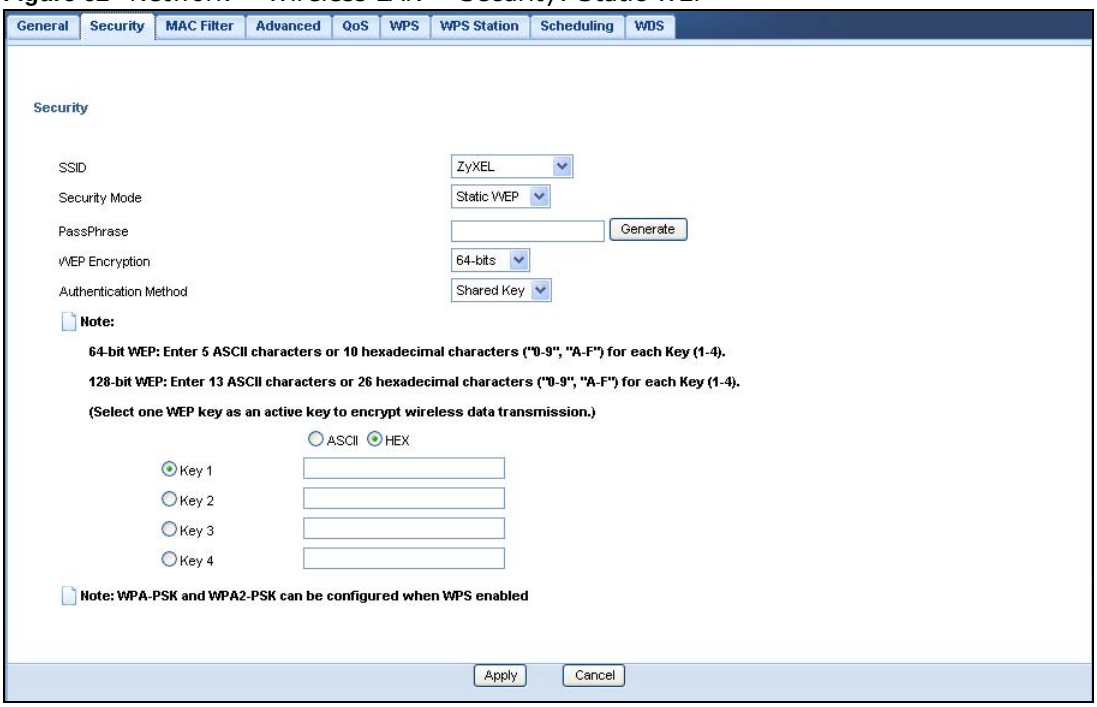
10.5.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your WAP3205 allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

Select **Static WEP** from the **Security Mode** list.

Figure 62 Network > Wireless LAN > Security: Static WEP



The following table describes the wireless LAN security labels in this screen.

Table 32 Network > Wireless LAN > Security: Static WEP

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure the security.
Security Mode	Select **Static WEP** to enable data encryption.
PassPhrase	Enter a Passphrase (up to 26 printable characters) and click Generate. A passphrase functions like a password. In WEP security mode, it is further converted by the WAP3205 into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.
WEP Encryption	Select **64-bits** or **128-bits**. This dictates the length of the security key that the network is going to use.
Authentication Method	Select **Auto** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** unless you want to force a key verification before communication between the wireless client and the WAP3205 occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

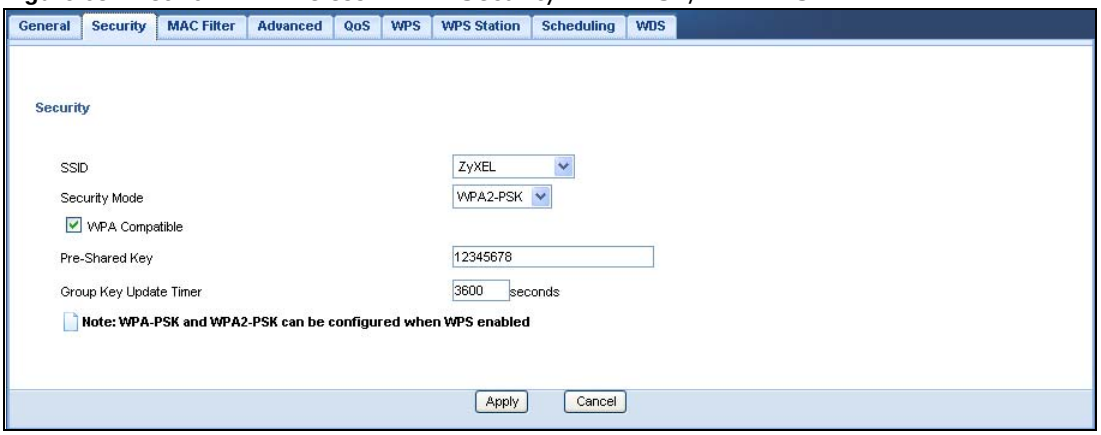
Table 32 Network > Wireless LAN > Security: Static WEP

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the WAP3205 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.5.3 WPA-PSK/WPA2-PSK

Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 63 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 33 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK

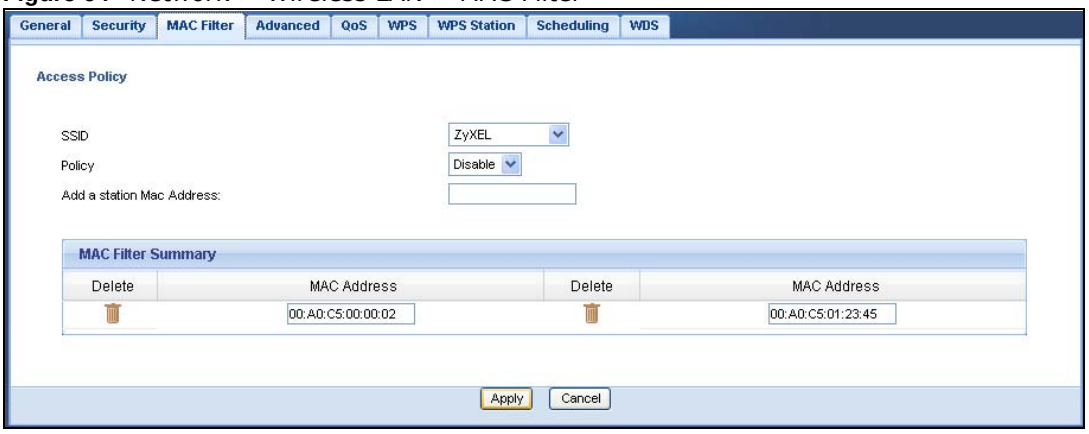
LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure the security.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** to enable data encryption.
WPA Compatible	This field appears when you choose **WPA2-PSK** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your WAP3205.
Pre-Shared Key	**WPA-PSK / WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The default is **3600** seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.6 MAC Filter

The MAC filter screen allows you to configure the WAP3205 to give exclusive access to devices (Allow) or exclude devices from accessing the WAP3205 (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your WAP3205's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 64 Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

Table 34 Network > Wireless LAN > MAC Filter

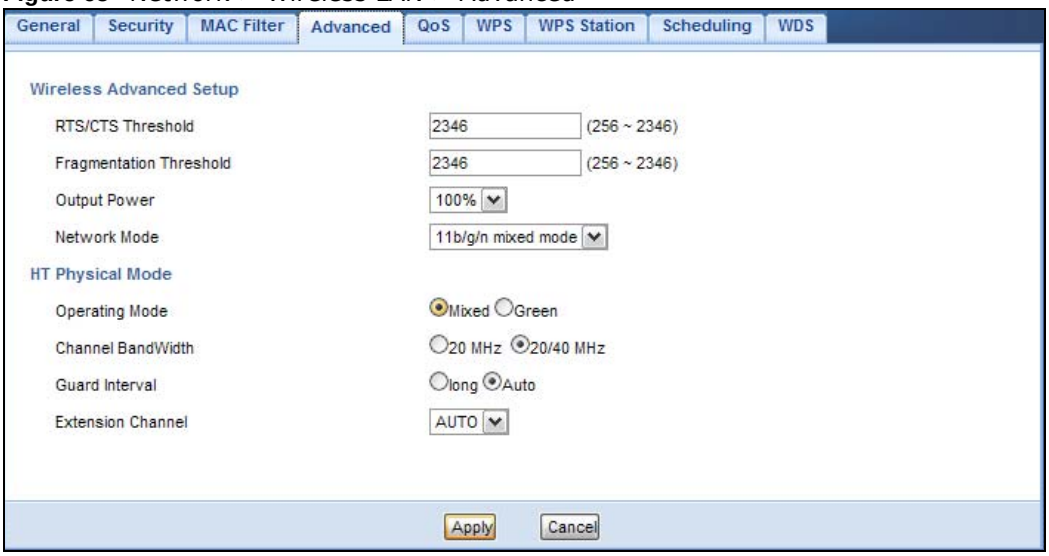
LABEL	DESCRIPTION
Access Policy	
SSID	Select the SSID for which you want to configure MAC filtering.
Policy	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to deactivate the MAC filtering rule you configure below. Select **Allow** to permit access to the WAP3205, MAC addresses not listed will be denied access to the WAP3205. Select **Reject** to block access to the WAP3205, MAC addresses not listed will be allowed to access the WAP3205
Add a station Mac Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the WAP3205 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
MAC Filter Summary	
Delete	Click the delete icon to remove the MAC address from the list.
MAC Address	This is the MAC address of the wireless station that are allowed or denied access to the WAP3205.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.7 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold and high-throughput physical mode settings.

Click **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 65 Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

Table 35 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 256 and 2432.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.
Output Power	Set the output power of the WAP3205 in this field. If there is a high density of APs in an area, decrease the output power of the WAP3205 to reduce interference with other APs. Select one of the following **100%**, **90%**, **75%**, **50%**, **25%** or **10%**. See the product specifications for more information on your WAP3205's output power.
Network Mode	Select **11b only** to allow only IEEE 802.11b compliant WLAN devices to associate with the WAP3205. Select **11g only** to allow only IEEE 802.11g compliant WLAN devices to associate with the WAP3205. Select **11 b/g mixed mode** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the WAP3205. The transmission rate of your WAP3205 might be reduced. Select **11 b/g/n mixed mode** to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the WAP3205. The transmission rate of your WAP3205 might be reduced.
HT (High Throughput) Physical Mode - Use the fields below to configure the 802.11 wireless environment of your WAP3205.	

Table 35 Network > Wireless LAN > Advanced

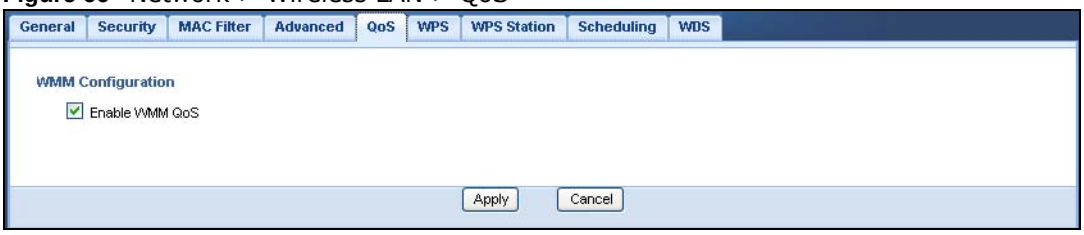
LABEL	DESCRIPTION
Operating Mode	Choose this according to the wireless mode(s) used in your network. **Mixed** - Select this if the wireless clients in your network use different wireless modes (for example, IEEE 802.11b/g and IEEE 802.1n modes) **Green** - Select this if the wireless clients in your network uses only one type of wireless mode (for example, IEEEE 802.11 n only)
Channel Bandwidth	Select the channel bandwidth you want to use for your wireless network. It is recommended that you select **20/40 MHz**. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
Guard Interval	Select **Auto** to increase data throughput. However, this may make data transfer more prone to errors. Select **Long** to prioritize data integrity. This may be because your wireless network is busy and congested or the WAP3205 is located in an environment prone to radio interference.
Extension Channel	This is set to **Auto** by default. If you select **20/40 MHz** as your **Channel Bandwidth**, the extension channel enables the WAP3205 to get higher data throughput. This also lowers radio interference and traffic.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.8 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

Click **Network** > **Wireless LAN** > **QoS**. The following screen appears.

Figure 66 Network > Wireless LAN > QoS



The following table describes the labels in this screen.

Table 36 Network > Wireless LAN > QoS

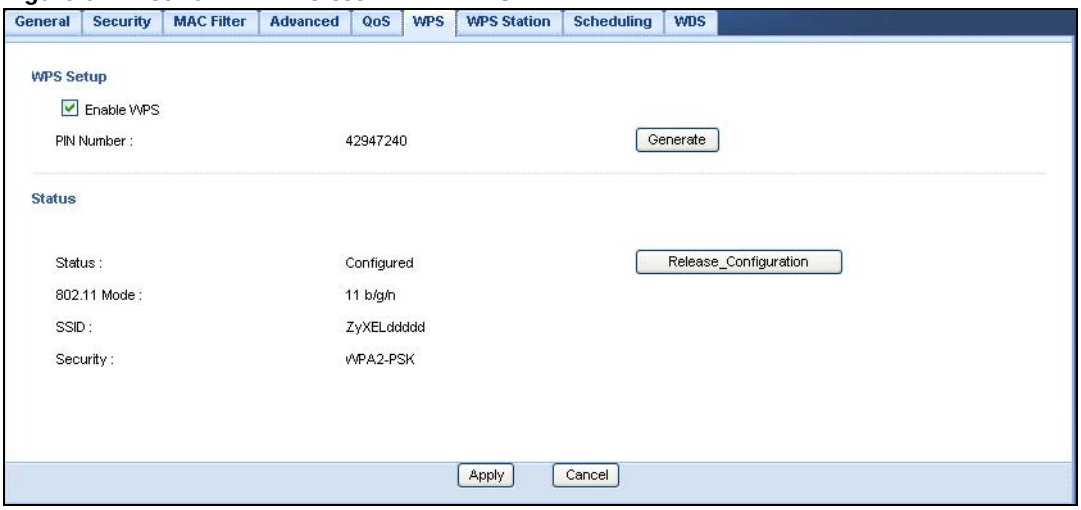
LABEL	DESCRIPTION
Enable WMM QoS	Check this to have the WAP3205 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click **Apply** to save your changes to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.9 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network** > **Wireless LAN** > **WPS** tab.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the WAP3205.

Figure 67 Network > Wireless LAN > WPS



The following table describes the labels in this screen.

Table 37 Network > Wireless LAN > WPS

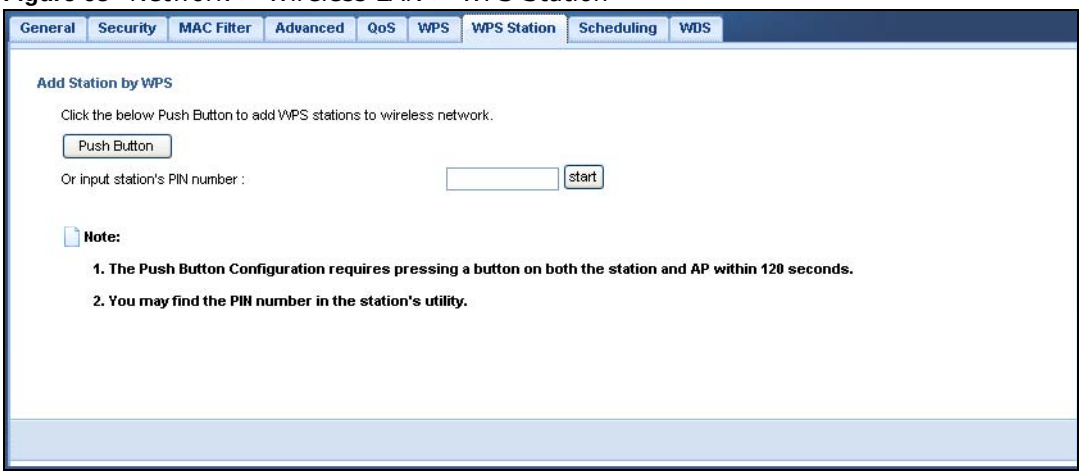
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
Status	
Status	This displays **Configured** when the WAP3205 has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the WAP3205 or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the WAP3205.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the WAP3205.
SSID	This is the name of the wireless network (the WAP3205's first SSID).
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.10 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN** > **WPS Station** tab.

Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 68 Network > Wireless LAN > WPS Station



The following table describes the labels in this screen.

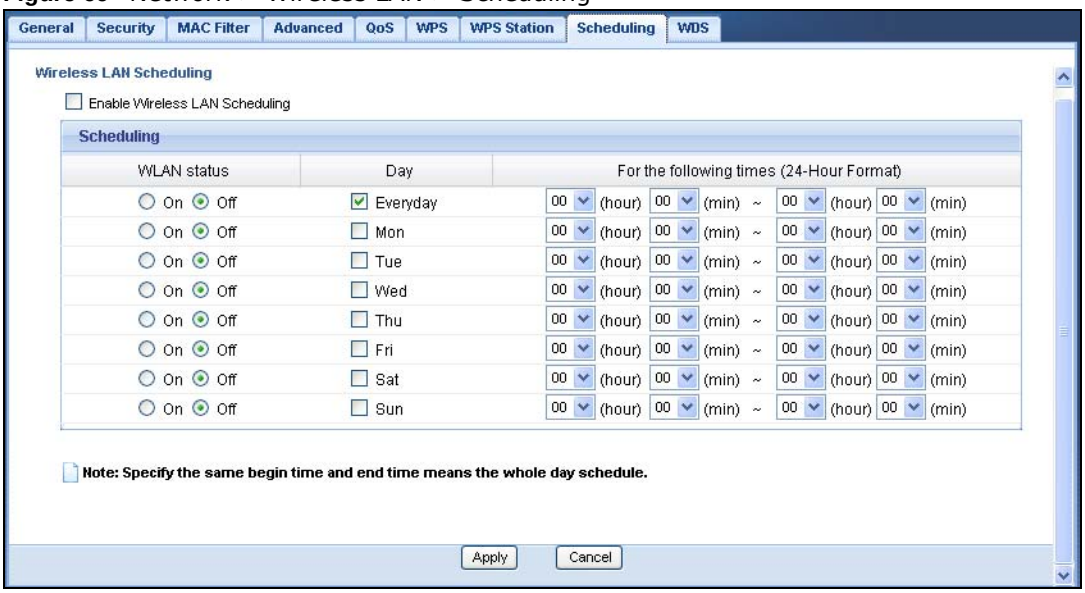
Table 38 Network > Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 8.3.1 on page 60. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 8.3.2 on page 61. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

10.11 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN** > **Scheduling** tab.

Figure 69 Network > Wireless LAN > Scheduling



The following table describes the labels in this screen.

Table 39 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Scheduling	
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **For the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **For the following times** field.
For the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click **Apply** to save your changes back to the WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

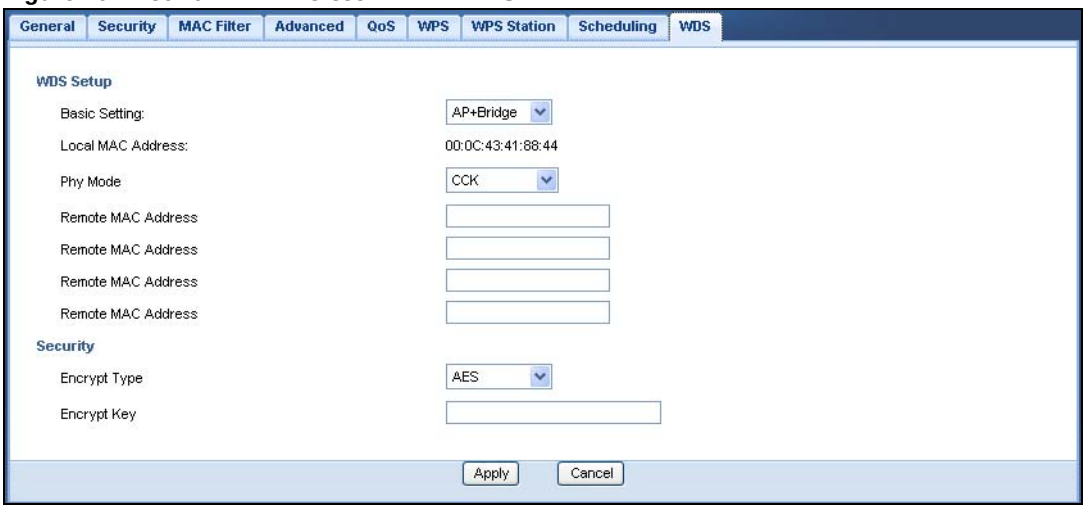
10.12 WDS Screen

A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Use this screen to set the operating mode of your WAP3205 to **AP + Bridge** or **Bridge** and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

Note: You must enable the same wireless security settings on the WAP3205 and on all wireless clients that you want to associate with it.

Click **Network** > **Wireless LAN** > **WDS** tab. The following screen opens with the **Basic Setting** set to **Disabled**, and **Security Mode** set to **No Security**.

Figure 70 Network > Wireless LAN > WDS



The following table describes the labels in this screen.

Table 40 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
WDS Setup	
Basic Settings	Select the operating mode for your WAP3205. • **Disable** - The WAP3205 works as an access point only and cannot establish wireless links with other APs. • **AP + Bridge -** The WAP3205 functions as a bridge and access point simultaneously. • **Bridge** - The WAP3205 acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The WAP3205 can establish up to five wireless links with other APs.
Local MAC Address	This is the MAC address of your WAP3205.
Phy Mode	Select the Phy mode you want the WAP3205 to use. This dictates the maximum size of packets during data transmission. This field is not available when you select **Disable** in the **Basic Setting** field.
Remote MAC Address	This is the MAC address of the peer device that your WAP3205 wants to make a bridge connection with. You can connect to up to 4 peer devices.
Security	
EncrypType	Select whether to use **WEP**, **TKIP** or **AES** encryption for your WDS connection in this field. Otherwise, select **No Security**.
EncrypKey	The **Encryp key** is used to encrypt data. Peers must use the same key for data transmission.

Table 40 Network > Wireless LAN > WDS

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to WAP3205.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11

LAN

11.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

Figure 71 LAN Example

The LAN screens can help you manage IP addresses.

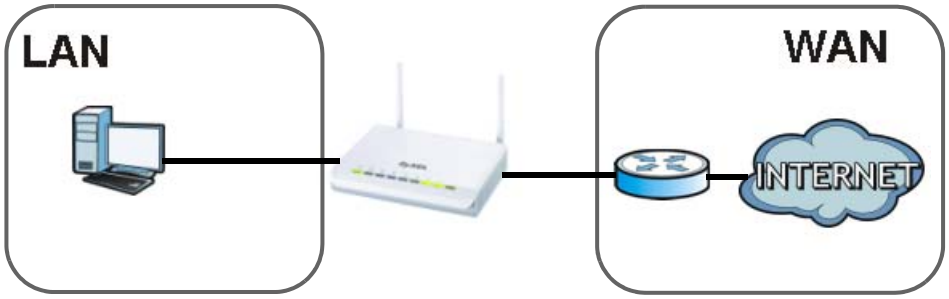
11.2 What You Can Do

- Use the **IP** screen (Section 11.4 on page 102) to change the IP address for your WAP3205 and DNS server information.
- Use the **IP Alias** screen (Section 11.5 on page 103) to have the WAP3205 apply IP alias to create LAN subnets.

11.3 What You Need To Know

There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 72 LAN and WAN IP Addresses



The LAN parameters of the WAP3205 are preset in the factory with the following values:

- IP address of 192.168.1.2 with subnet mask of 255.255.255.0 (24 bits)

11.3.1 LAN TCP/IP

The WAP3205 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

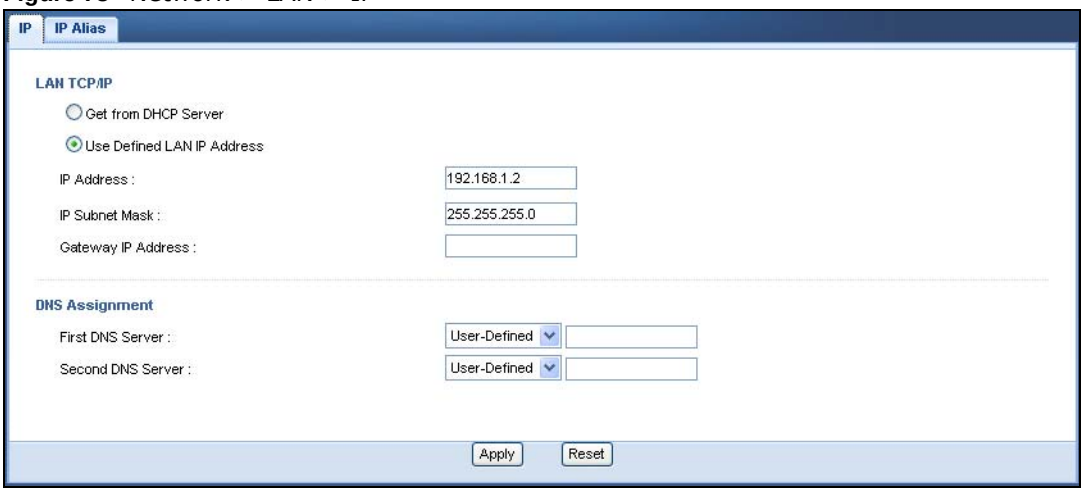
11.3.2 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The WAP3205 supports three logical LAN interfaces via its single physical Ethernet interface with the WAP3205 itself as the gateway for each LAN network.

11.4 LAN IP Screen

Use this screen to change the IP address for your WAP3205. Click **Network > LAN > IP**.

Figure 73 Network > LAN > IP



The following table describes the labels in this screen.

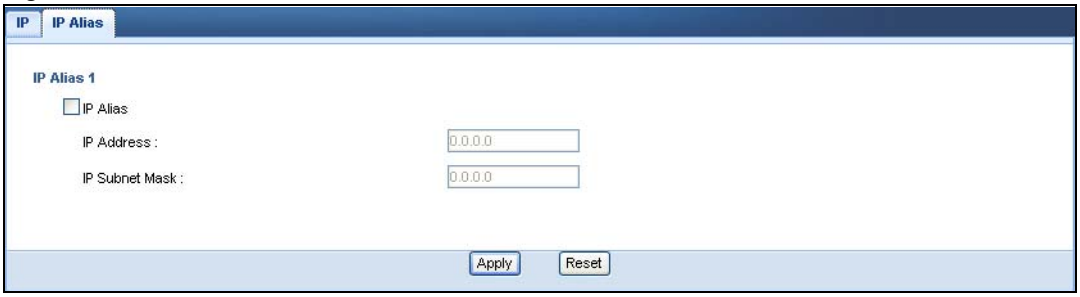
Table 41 Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	Click this to deploy the WAP3205 as a DHCP client in the network. When you enable this, the WAP3205 gets its IP address from the network's DHCP server (for example, your ISP or router). Users connected to the WAP3205 can now access the network (i.e., the Internet if the IP address is given by the ISP or a router with Internet access). The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the WAP3205. Otherwise, you need to reset the WAP3205 to be able to access the Web Configurator again (see Section 12.7 on page 110 for details on how to reset the WAP3205). Also when you select this, you cannot enter an IP address for your WAP3205 in the field below.
Use Defined LAN IP Address	Click this if you want to specify the IP address of your WAP3205. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Gateway IP Address	Enter a gateway IP address (if your ISP or network administrator gave you one) in this field.
DNS Assignment	
First DNS Server Second DNS Server	Select **From ISP** if your ISP or router to which the WAP3205 connects dynamically assigns DNS server information (and the WAP3205's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 IP Alias Screen

Use this screen to have the WAP3205 apply IP alias to create LAN subnets. Click **LAN** > **IP Alias**.

Figure 74 Network > LAN > IP Alias



The following table describes the labels in this screen.

Table 42 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias	Check this to enable IP alias.
IP Address	Type the IP alias address of your WAP3205 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to begin configuring this screen afresh.

12

Maintenance

12.1 Overview

This chapter provides information on the **Maintenance** screens.

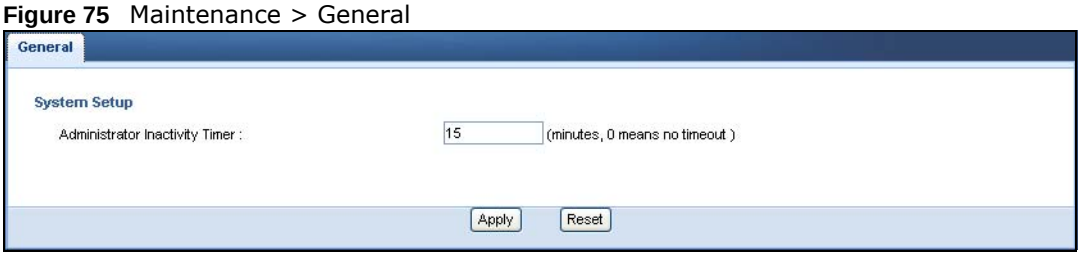
12.2 What You Can Do

- Use the **General** screen (Section 12.3 on page 105) to set the timeout period of the management session.
- Use the **Password** screen (Section 12.4 on page 106) to change your WAP3205's system password.
- Use the **Time** screen (Section 12.5 on page 107) to change your WAP3205's time and date.
- Use the **Firmware Upgrade** screen (Section 12.6 on page 109) to upload firmware to your WAP3205.
- Use the **Backup/Restore** screen (Section 12.8 on page 111) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use the **Reset/Restart** screen (Section 12.8 on page 111) to reboot the WAP3205 without turning the power off.
- Use the **Sys OP Mode** screen (Section 12.10 on page 113) to select how you want to use your WAP3205.

12.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance** > **General**. The following screen displays.

Figure 75 Maintenance > General



The following table describes the labels in this screen.

Table 43 Maintenance > General

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to begin configuring this screen afresh.

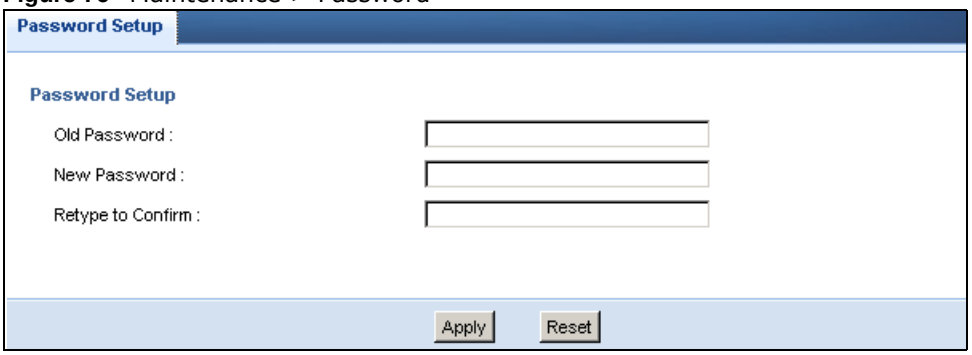
12.4 Password Screen

It is strongly recommended that you change your WAP3205's password.

If you forget your WAP3205's password (or IP address), you will need to reset the device. See Section 12.8 on page 111 for details

Click **Maintenance** > **Password**.

Figure 76 Maintenance > Password



The following table describes the labels in this screen.

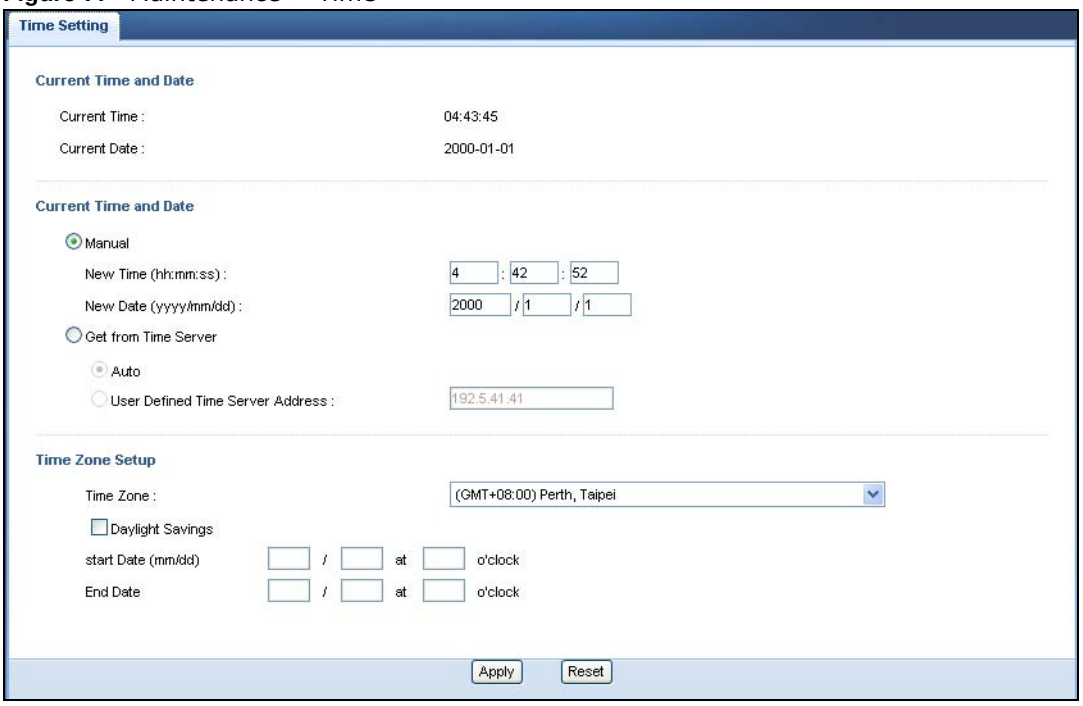
Table 44 Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your WAP3205’s password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to begin configuring this screen afresh.

12.5 Time Setting Screen

Use this screen to configure the WAP3205's time based on your local time zone. To change your WAP3205's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 77 Maintenance > Time



he following table describes the labels in this screen.

Table 45 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your WAP3205. Each time you reload this page, the WAP3205 synchronizes the time with the time server.
Current Date	This field displays the date of your WAP3205. Each time you reload this page, the WAP3205 synchronizes the date with the time server.
Current Time and Date	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select **Manual**, enter the new time in this field and then click **Apply**.

Table 45 Maintenance > Time

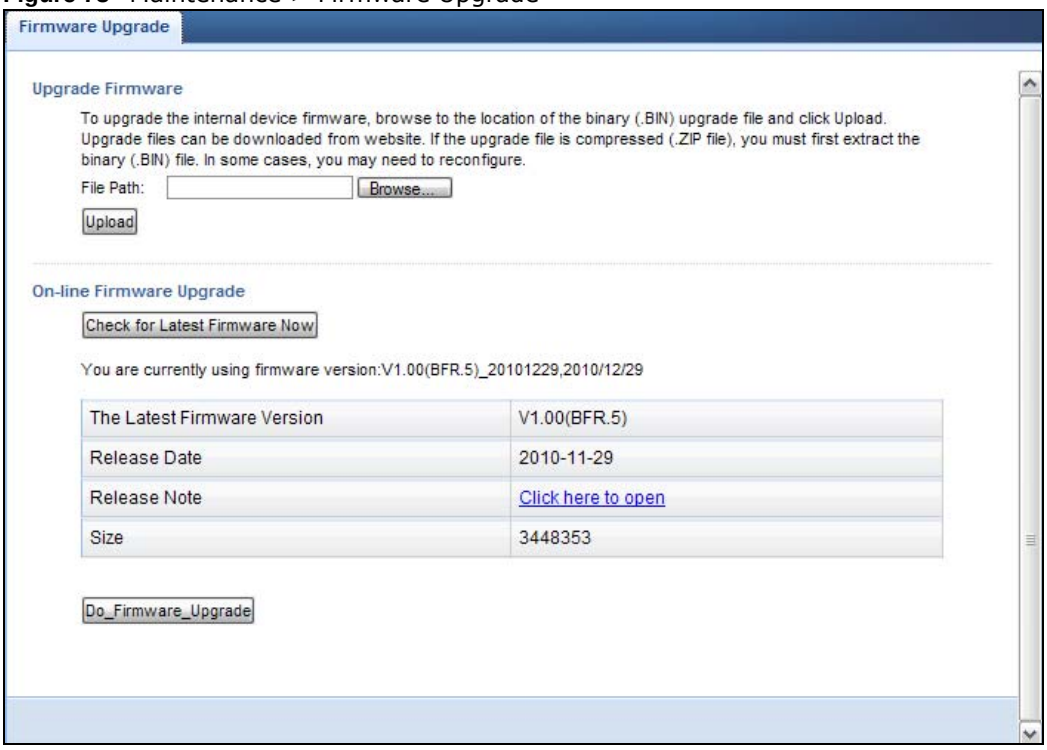
LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the WAP3205 get the time and date from the time server you specified below.
Auto	Select **Auto** to have the WAP3205 automatically search for an available time server and synchronize the date and time with the time server after you click **Apply**.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the WAP3205.
Reset	Click **Reset** to begin configuring this screen afresh.

12.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "WAP3205.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your WAP3205.

Figure 78 Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

Table 46 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
On-line Firmware Upgrade	
Check for Latest Firmware Now	Click this button to get the latest firmware information, such as the version number, release date, release note and file size from the ZyXEL website. Make sure your WAP3205 has Internet access.
Do-Firmware_Upgrade	Click this button to download and install the latest firmware in your WAP3205.

Note: Do not turn off the WAP3205 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the WAP3205 again.

The WAP3205 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 79 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

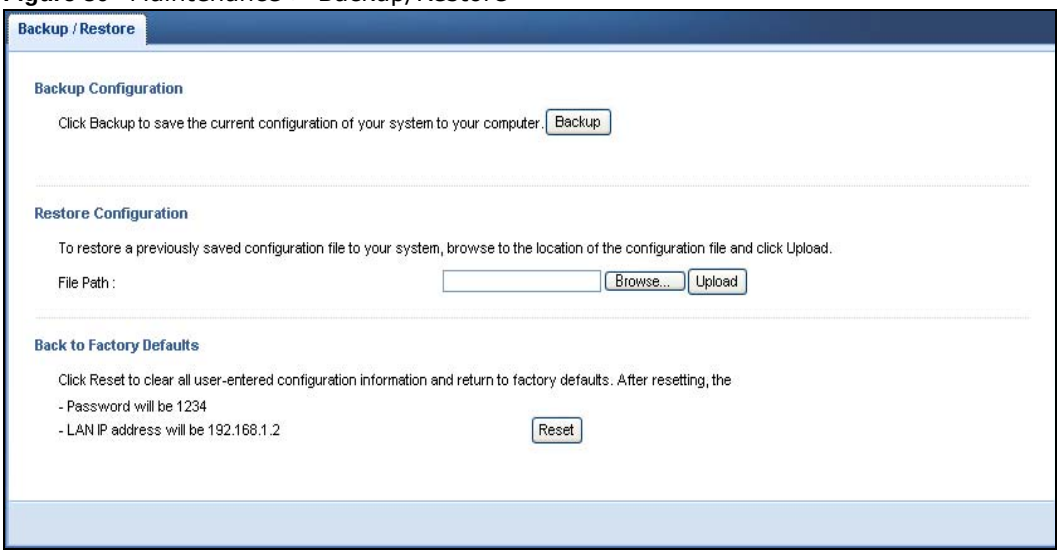
12.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the WAP3205's current configuration to a file on your computer. Once your WAP3205 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your WAP3205.

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 80 Maintenance > Backup/Restore



The following table describes the labels in this screen.

Table 47 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click **Backup** to save the WAP3205's current configuration to your computer.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the WAP3205 while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the WAP3205 again. The WAP3205 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the WAP3205 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your WAP3205. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

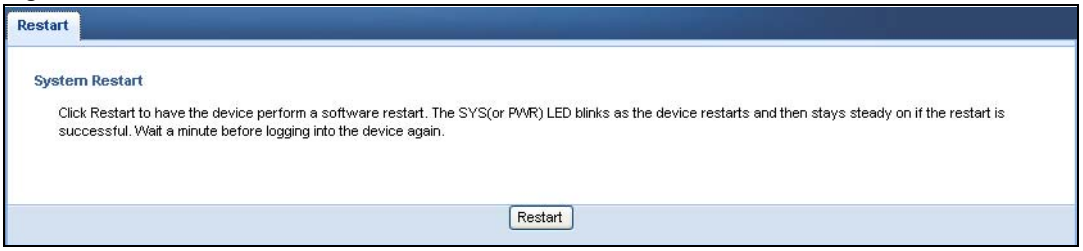
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default WAP3205 IP address (192.168.1.2). See Appendix C on page 141 for details on how to set up your computer's IP address.

12.8 Reset/Restart Screen

System restart allows you to reboot the WAP3205 without turning the power off.

Click **Maintenance > Reset/Restart** to open the following screen.

Figure 81 Maintenance > Reset/Restart



Click **Restart** to have the WAP3205 reboot. This does not affect the WAP3205's configuration.

12.9 System Operation Mode Overview

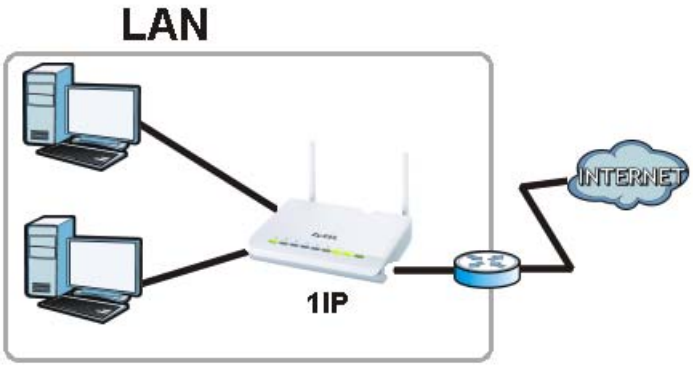
The **Sys OP Mode** (System Operation Mode) function lets you configure your WAP3205 as an access point, wireless client or both at the same time. You can choose between **Access Point Mode**, **Client Mode** and **Universal Repeater Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your WAP3205.

Access Point

An access point enabled all ethernet ports to be bridged together and be in the same subnet. To connect to the Internet, another device, such as a router, is required.

Figure 82 Access Point Mode



Client

WAP3205 in client mode connects to an existing access point wirelessly. It acts just like a wireless client in notebooks/computers.

Figure 83 Client Mode

Universal Repeater

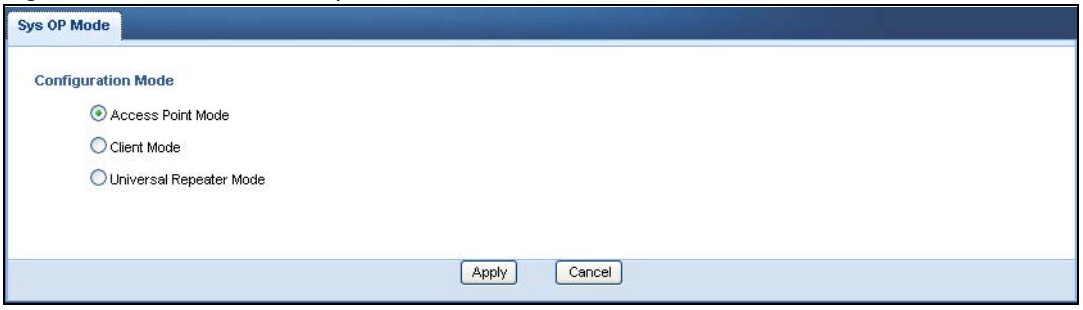
WAP3205 in Universal Repeater mode work as an access point and wireless client simutaneously.

Figure 84 Universal Repeater Mode

12.10 Sys Op Mode Screen

Use this screen to select how you want to use your WAP3205.

Figure 85 Maintenance > Sys OP Mode



The following table describes the labels in the **General** screen.

Table 48 Maintenance > Sys OP Mode

LABEL	DESCRIPTION
System Operation Mode	
Access Point	Select **Access Point Mode** if your device bridges traffic between clients on the same network. • In Access Point mode all Ethernet ports have the same IP address. • The default IP address of the device on the local network is 192.168.1.2.
Client Mode	Select **Client Mode** if your device needs a wireless client to connect to an existing access point. • You cannot configure wireless LAN settings like MAC filtering, QoS, WDS and scheduling in the client mode. • The IP address of the device on the local network is the same as the IP address given to the WAP3205 while in access point mode (default is 192.168.1.2).
Universal Repeater Mode	Select **Universal Repeater Mode** if you want to have wireless clients associate with the WAP3205 and also want to connect the WAP3205 to an existing access point. • In addition to wireless LAN settings between the WAP3205 and wireless clients, you also need to configure security and wireless settings between the WAP3205 and another access point. • WDS is not available when the WAP3205 is in universal repeater mode. • The IP address of the device on the local network is the same as the IP address given to the WAP3205 while in access point mode (default is 192.168.1.2).

LABEL	DESCRIPTION
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return your settings to the default (**Router**)

Note: If you select the incorrect System Operation Mode you may not be able to connect to the Internet.

13

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- WAP3205 Access and Login
- Internet Access
- Resetting the WAP3205 to Its Factory Defaults
- Wireless Router/AP Troubleshooting

13.1 Power, Hardware Connections, and LEDs

The WAP3205 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the WAP3205.
2. Make sure the power adaptor or cord is connected to the WAP3205 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the WAP3205.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 12.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the WAP3205.
5. If the problem continues, contact the vendor.

13.2 WAP3205 Access and Login

I don't know the IP address of my WAP3205.

1. The default IP address is **192.168.1.2**.
2. If you changed the IP address and have forgotten it,
   - and your WAP3205 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
   - reset your WAP3205 to change all settings back to their default. This means your current settings are lost. See Section 13.4 on page 118 in the **Troubleshooting** for information on resetting your WAP3205.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 13.4 on page 118.

I cannot see or access the **Login** screen in the Web Configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.2.
   - If you changed the IP address (Section 11.4 on page 102), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my WAP3205.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix A on page 121.
4. Make sure your computer is in the same subnet as the WAP3205. (If you know that there are routers between your computer and the WAP3205, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 11.4 on page 102.
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the WAP3205. See Appendix B on page 131.

5 Reset the device to its factory defaults, and try to access the WAP3205 with the default IP address. See Section 12.7 on page 110.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestion

- If your computer is connected wirelessly, use a computer that is connected to a **LAN** port.

I can see the **Login** screen, but I cannot log in to the WAP3205.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

3 Disconnect and re-connect the power adaptor or cord to the WAP3205.

4 If this does not work, you have to reset the device to its factory defaults. See Section 13.4 on page 118.

13.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

2 Make sure the WAP3205 is connected to a broadband modem or router with Internet access.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

- Go to **Network > Wireless LAN > General > WDS** and check if the WAP3205 is set to bridge mode. Select **Disable** and try to connect to the Internet again.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 Go to **Maintenance > Sys OP Mode**. Check your System Operation Mode setting.

- Select **Access Point Mode** if your WAP3205 bridges traffic between clients on the same network.
- Select **Client Mode** if your WAP3205 needs a wireless client to connect to an existing access point.

- Select **Universal Repeater Mode** if you want to have wireless clients associate with the WAP3205 and also want to connect the WAP3205 to an existing access point.

6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the WAP3205), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 12.

2 Reboot the WAP3205.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 12. If the WAP3205 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving the clients closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Reboot the WAP3205.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it.

13.4 Resetting the WAP3205 to Its Factory Defaults

If you reset the WAP3205, you lose all of the changes you have made. The WAP3205 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the WAP3205,

1 Make sure the power LED is on.

2 Press the **RESET** button for longer than 1 second to restart/reboot the WAP3205.

3 Press the **RESET** button for longer than five seconds to set the WAP3205 back to its factory-default configurations.

If the WAP3205 restarts automatically, wait for the WAP3205 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the WAP3205 does not restart automatically, disconnect and reconnect the WAP3205's power. Then, follow the directions above again.

13.5 Wireless Router/AP Troubleshooting

I cannot access the WAP3205 or ping any computer from the WLAN (wireless AP or router).

1 Make sure the wireless adapter on the wireless station is working properly.

2 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the WAP3205.

3 Make sure your computer (with a wireless adapter installed) is within the transmission range of the WAP3205.

4 Check that both the WAP3205 and your wireless station are using the same wireless and wireless security settings.

A

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

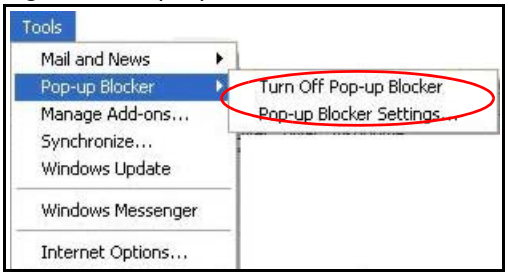
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 86 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 87 Internet Options: Privacy

3 Click **Apply** to save this setting.

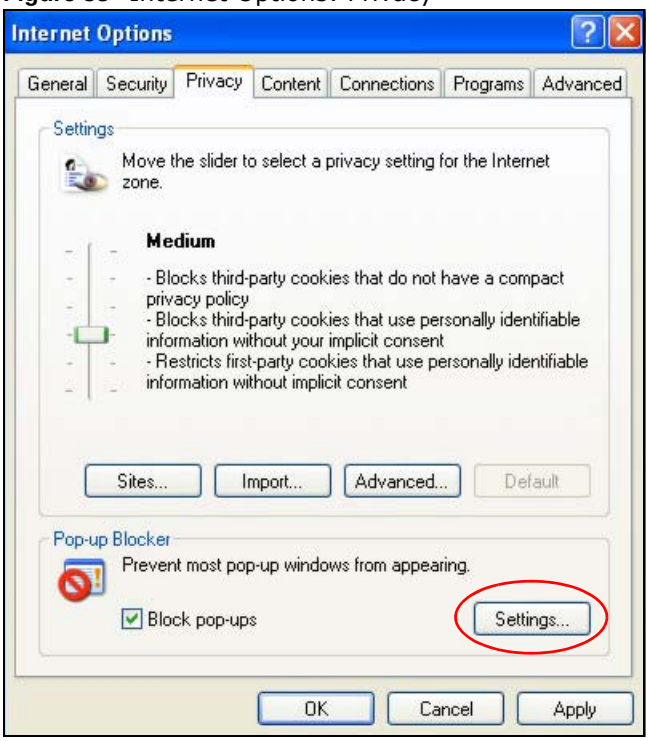
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

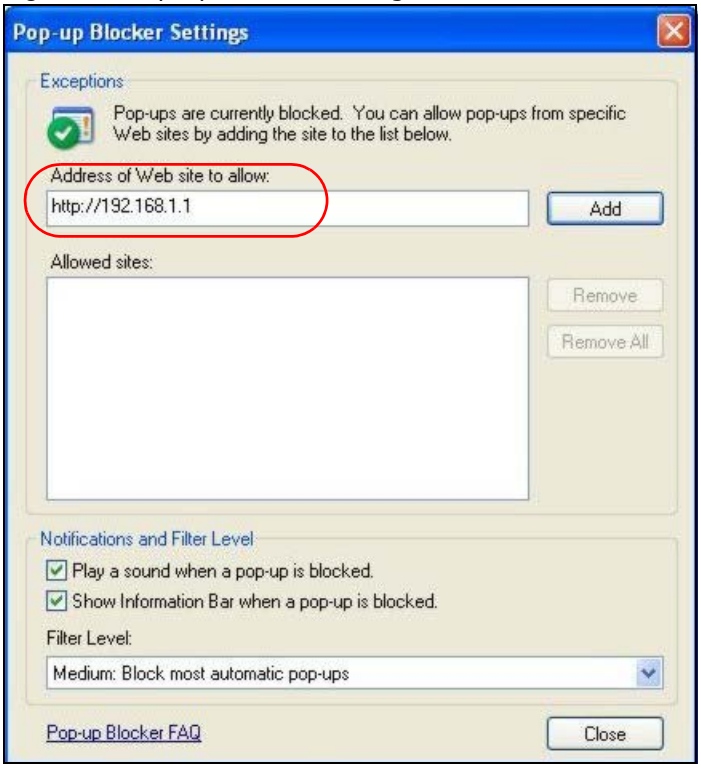
Figure 88 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 89 Pop-up Blocker Settings



5 Click **Close** to return to the **Privacy** screen.

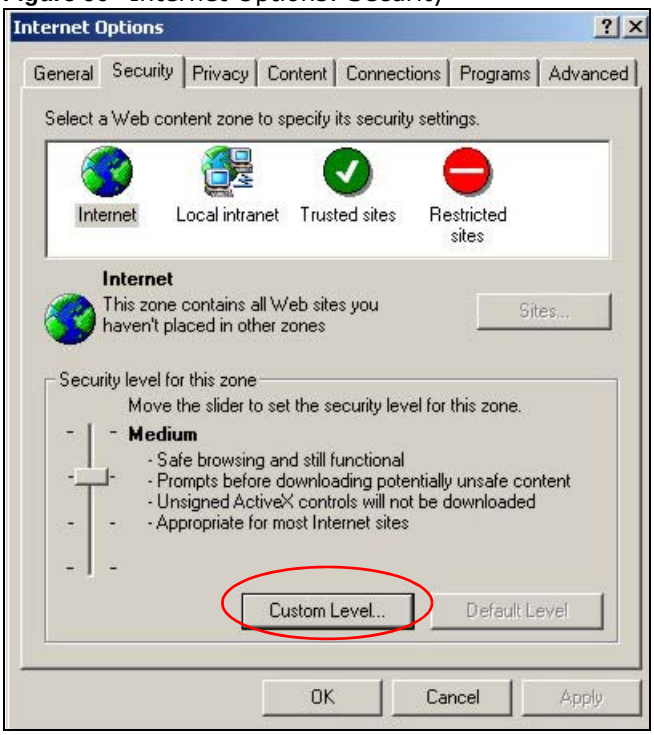
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 90 Internet Options: Security



2 Click the **Custom Level...** button.

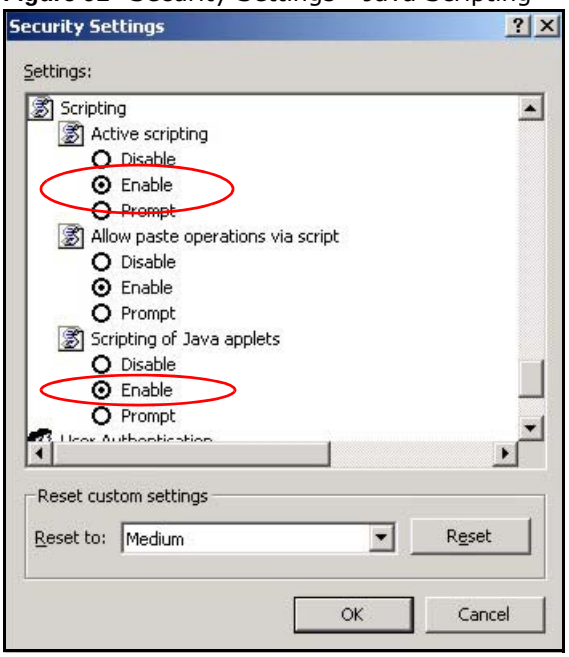
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 91 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

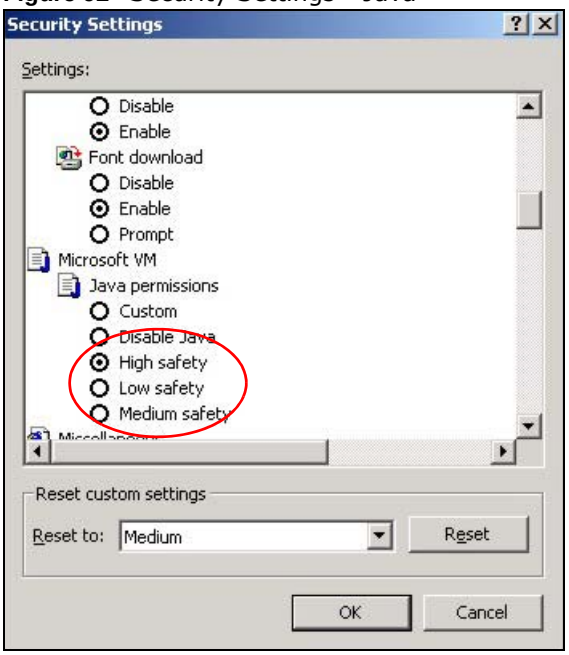
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 92 Security Settings - Java



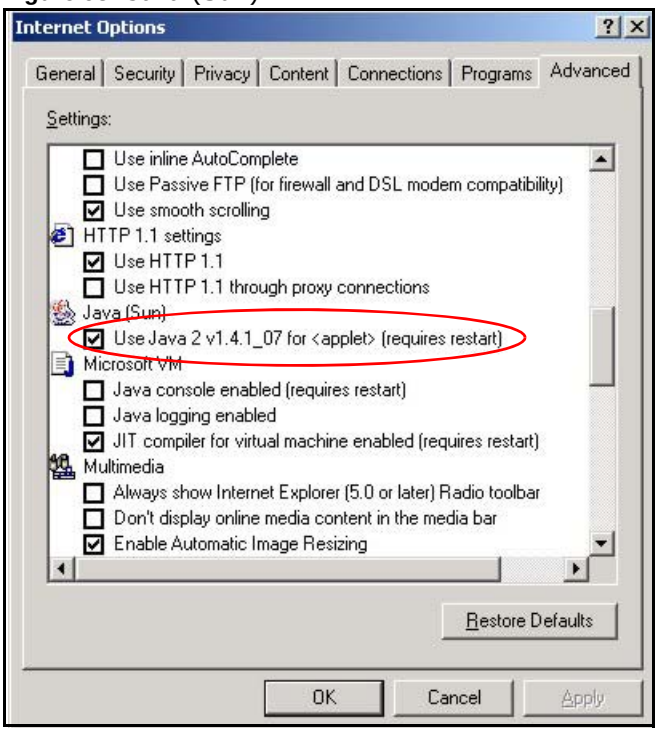
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 93 Java (Sun)

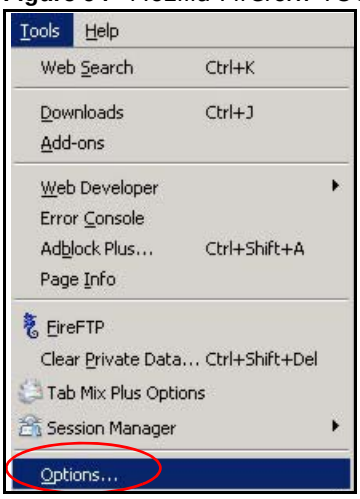


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

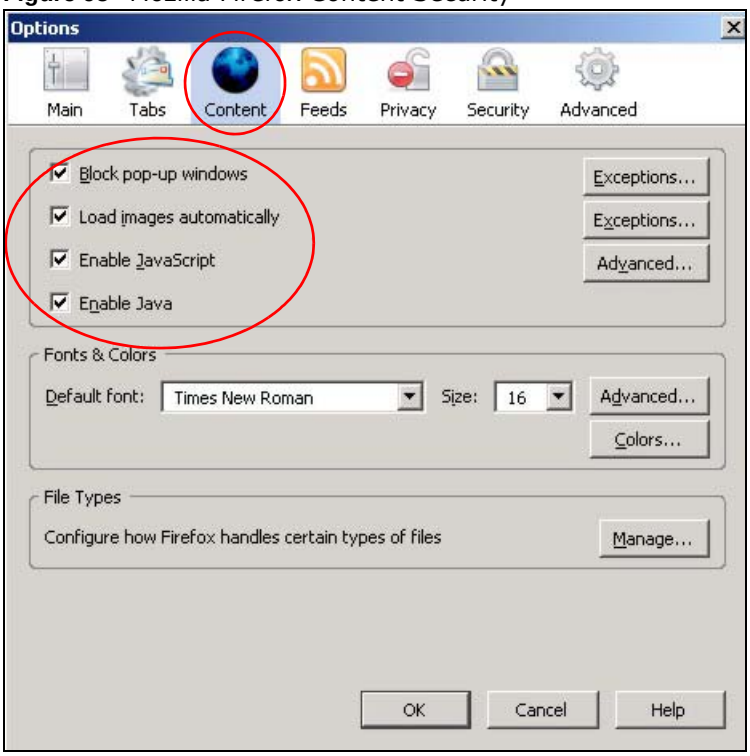
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 94 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 95 Mozilla Firefox Content Security



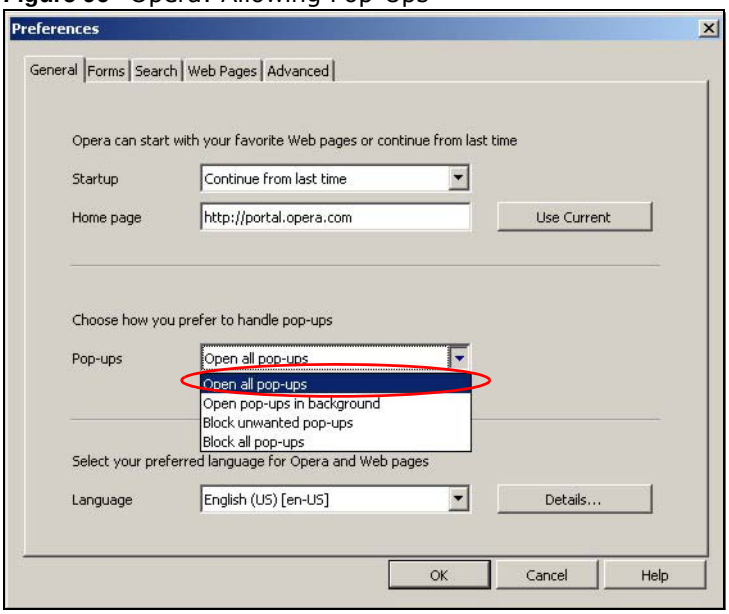
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

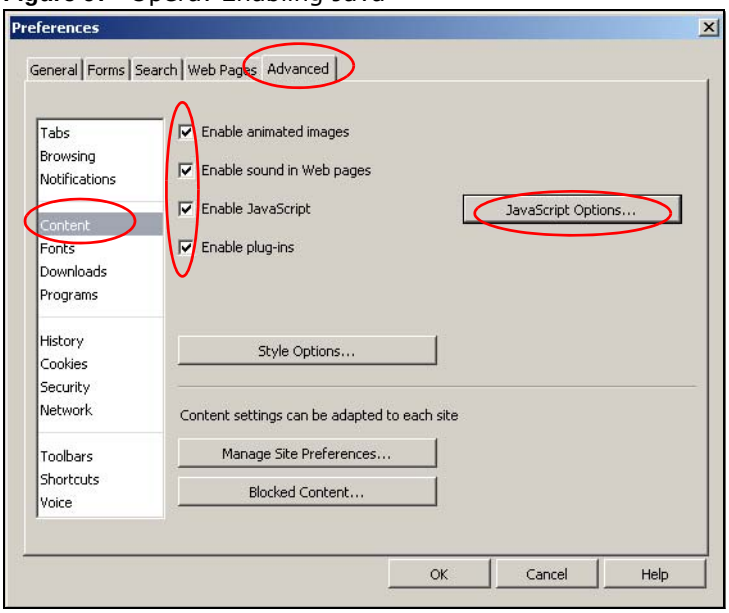
Figure 96 Opera: Allowing Pop-Ups



Enabling Java

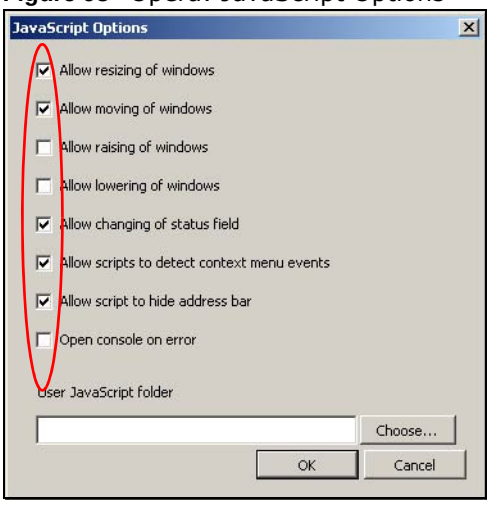
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 97 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 98 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

B

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

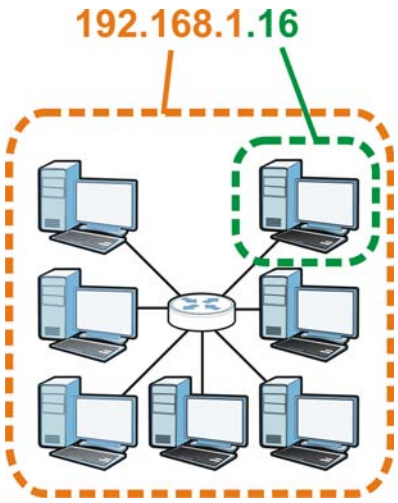
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 99 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 49 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 50 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 51 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 52 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192

Table 52 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

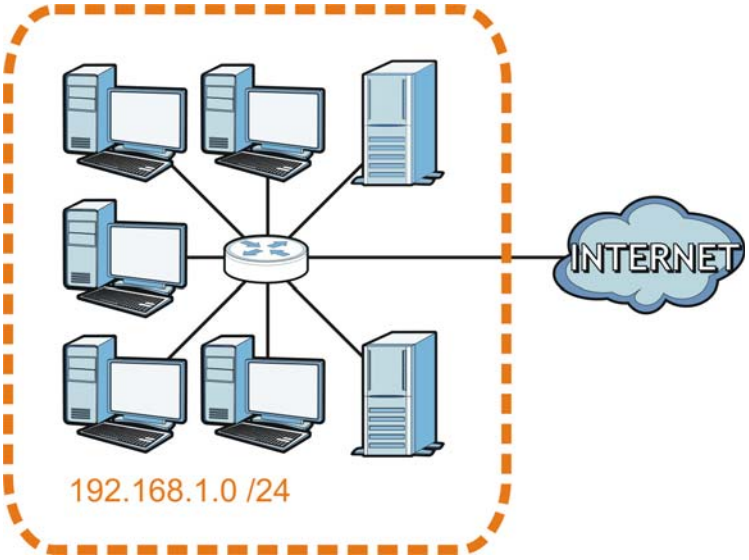
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 100 Subnetting Example: Before Subnetting

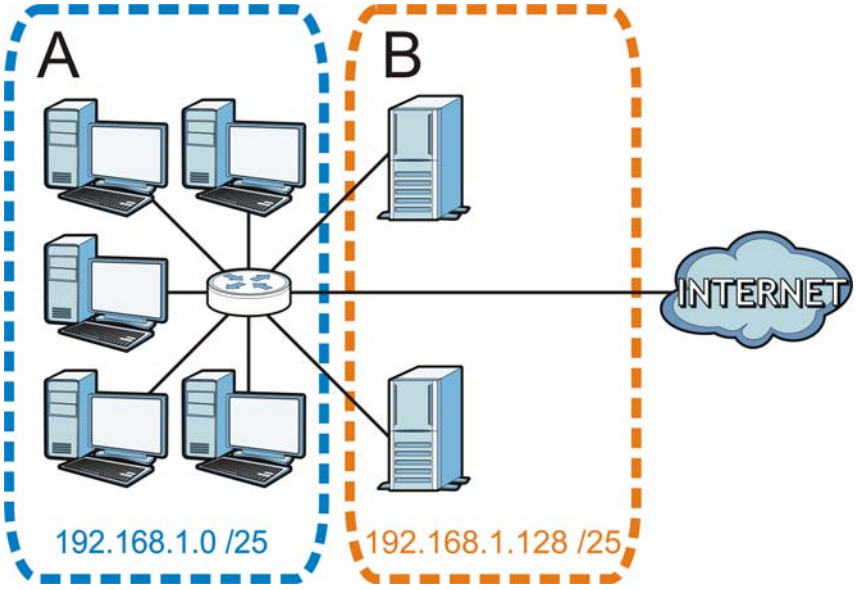


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 101 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 53 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 54 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 55 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 56 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 57 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191

Table 57 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 58 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 59 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the WAP3205.

Once you have decided on the network number, pick an IP address for your WAP3205 that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your WAP3205 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the WAP3205 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

IP Address Conflicts

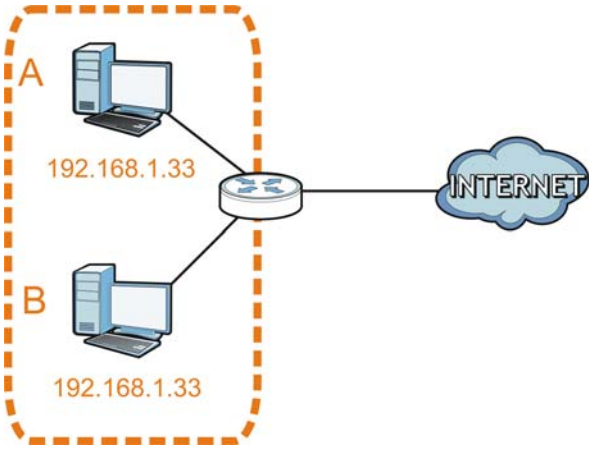
Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to

computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

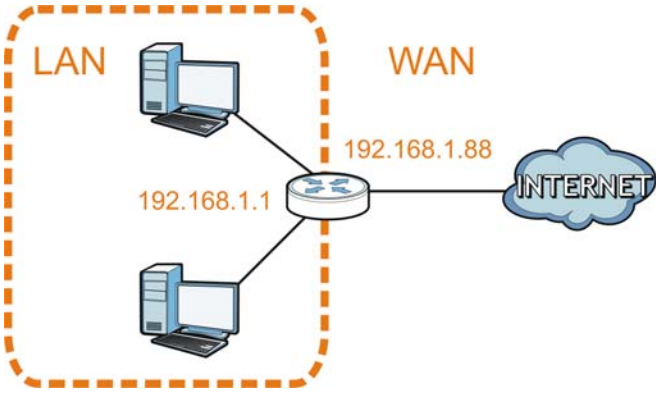
Figure 102 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

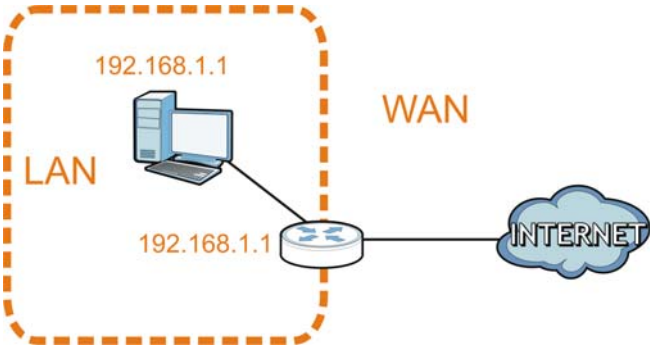
Figure 103 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 104 Conflicting Computer and Router IP Addresses Example



C

Setting Up Your Computer's IP Address

Note: Your specific WAP3205 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

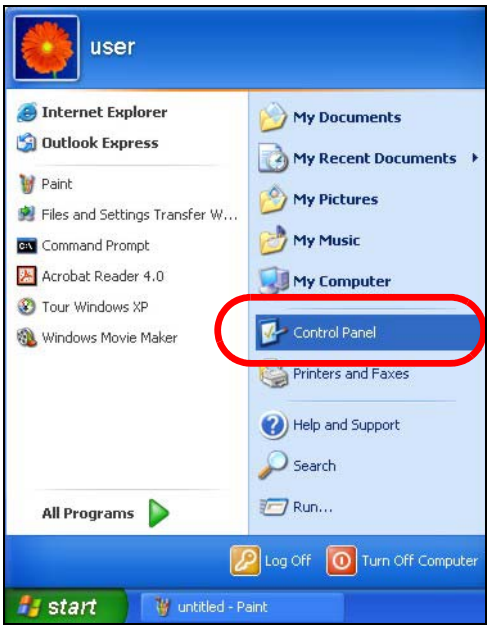
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 141
- Windows Vista on page 145
- Windows 7 on page 149
- Mac OS X: 10.3 and 10.4 on page 153
- Mac OS X: 10.5 and 10.6 on page 156
- Linux: Ubuntu 8 (GNOME) on page 159
- Linux: openSUSE 10.3 (KDE) on page 163

Windows XP/NT/2000

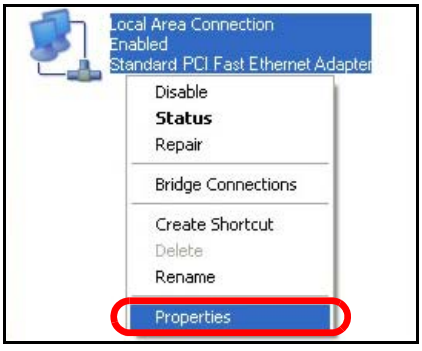
The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

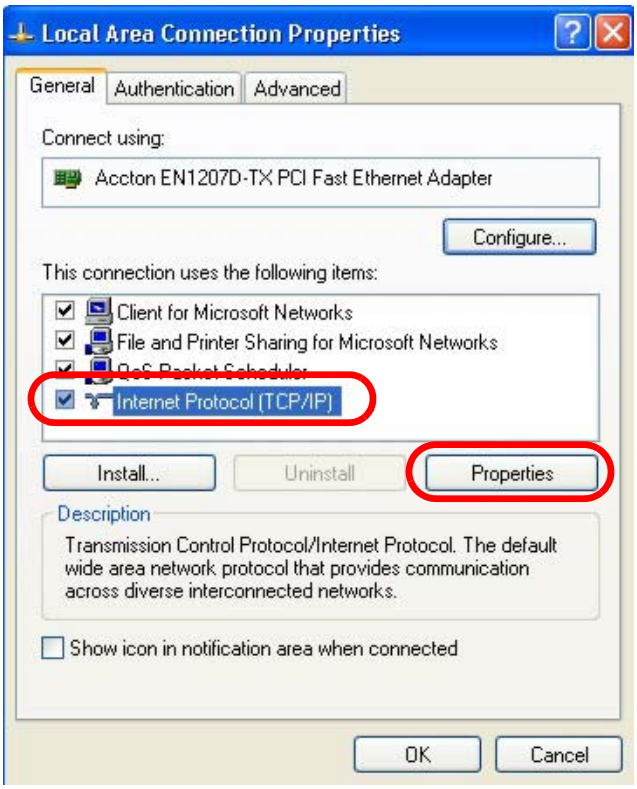


2 In the **Control Panel**, click the **Network Connections** icon.

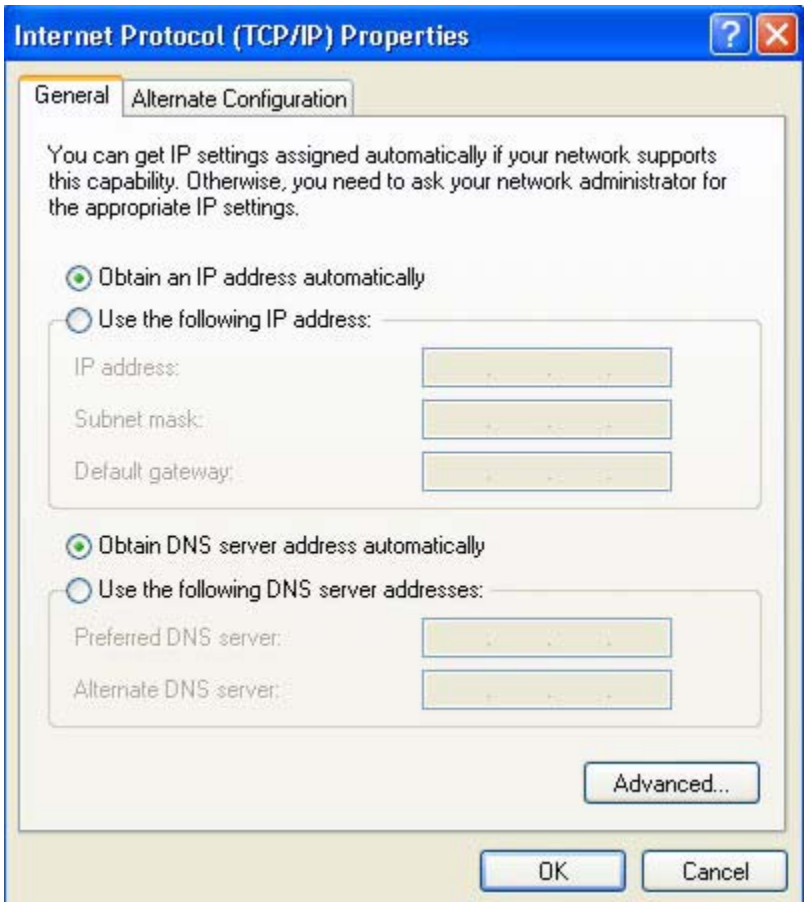
3 Right-click **Local Area Connection** and then select **Properties**.



4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



5 The **Internet Protocol TCP/IP Properties** window opens.



6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

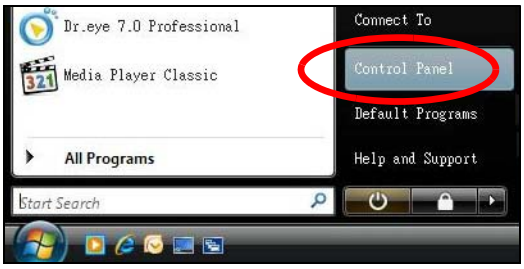
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

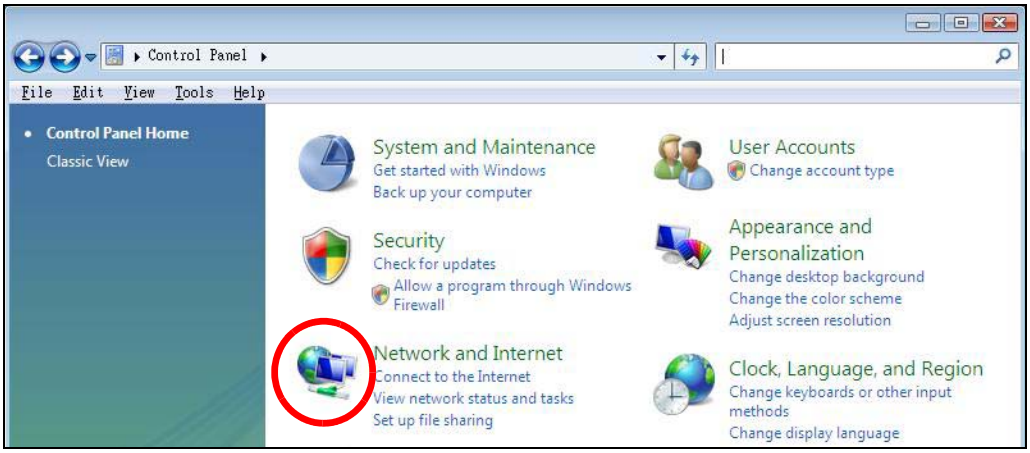
Windows Vista

This section shows screens from Windows Vista Professional.

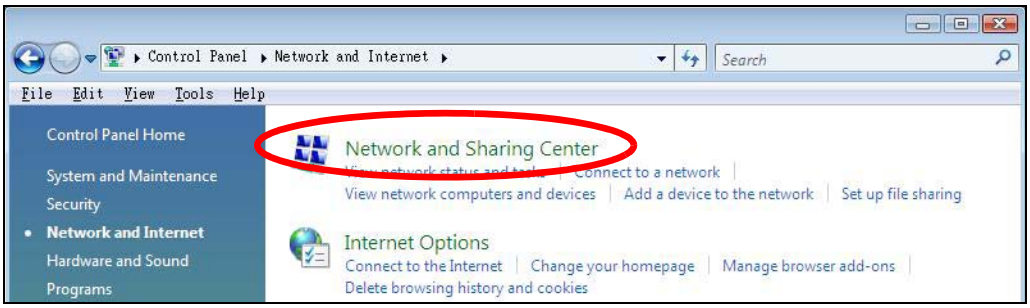
1 Click **Start** > **Control Panel**.



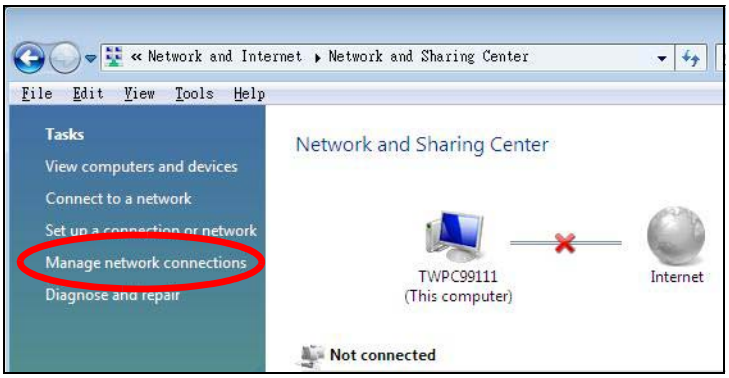
2 In the **Control Panel**, click the **Network and Internet** icon.



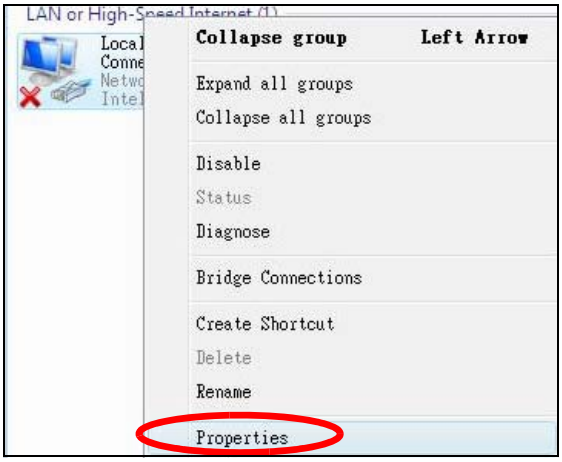
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

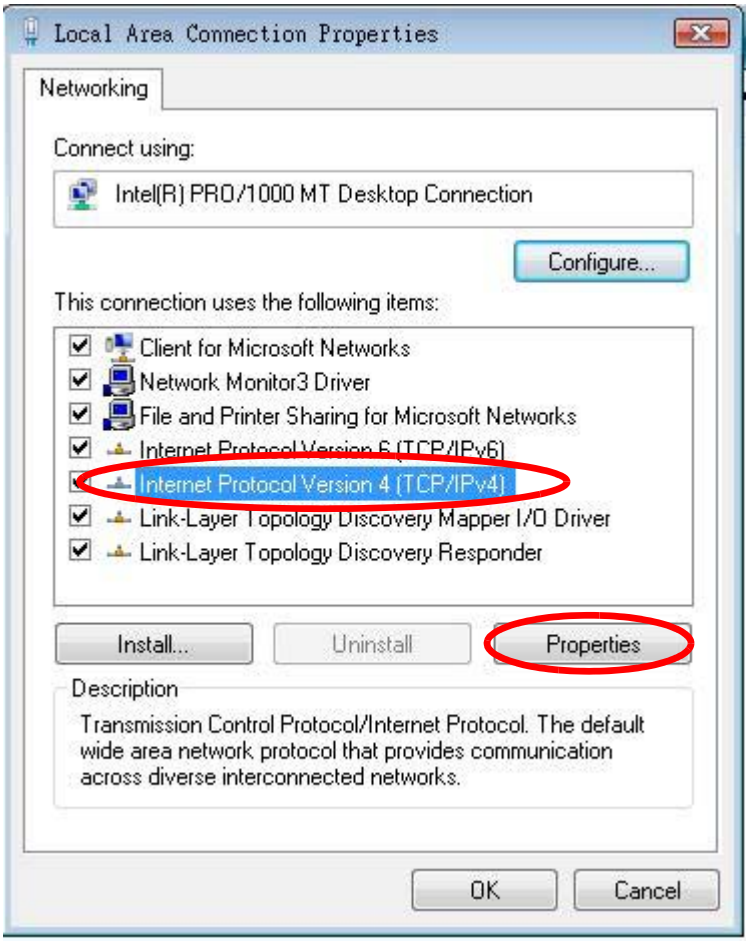


5 Right-click **Local Area Connection** and then select **Properties**.

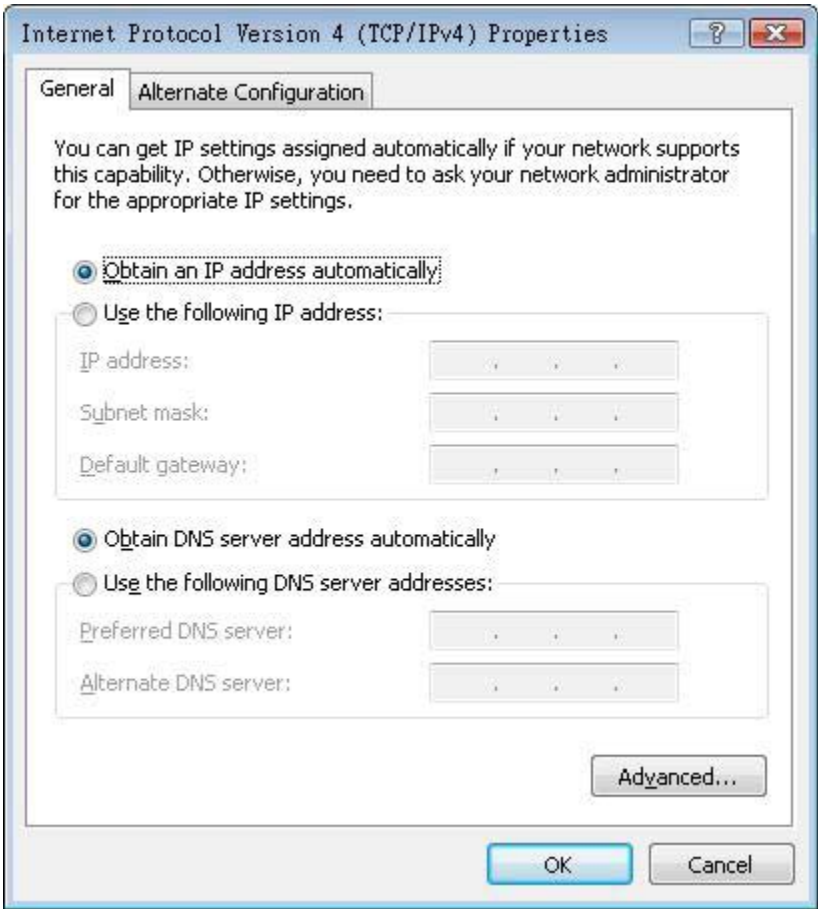


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

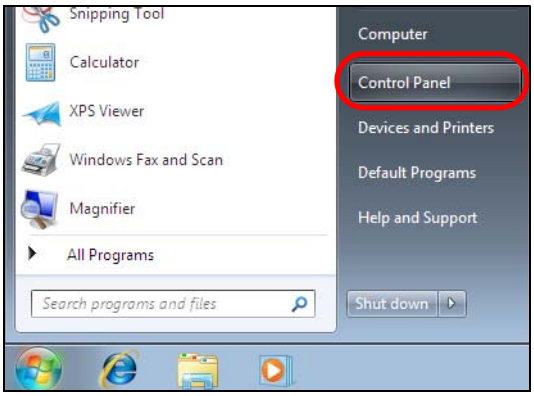
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

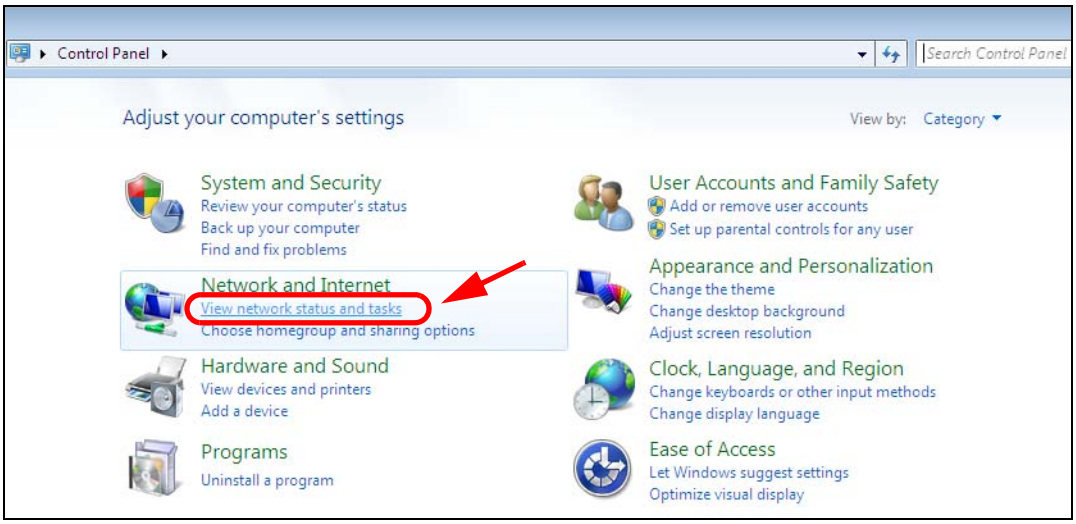
Windows 7

This section shows screens from Windows 7 Enterprise.

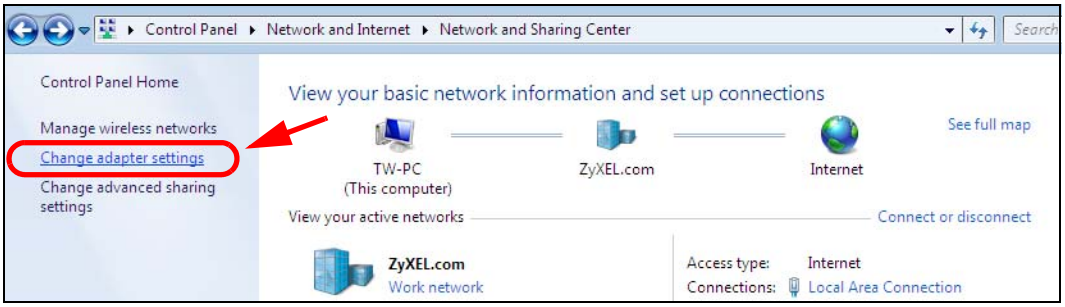
1 Click **Start** > **Control Panel**.



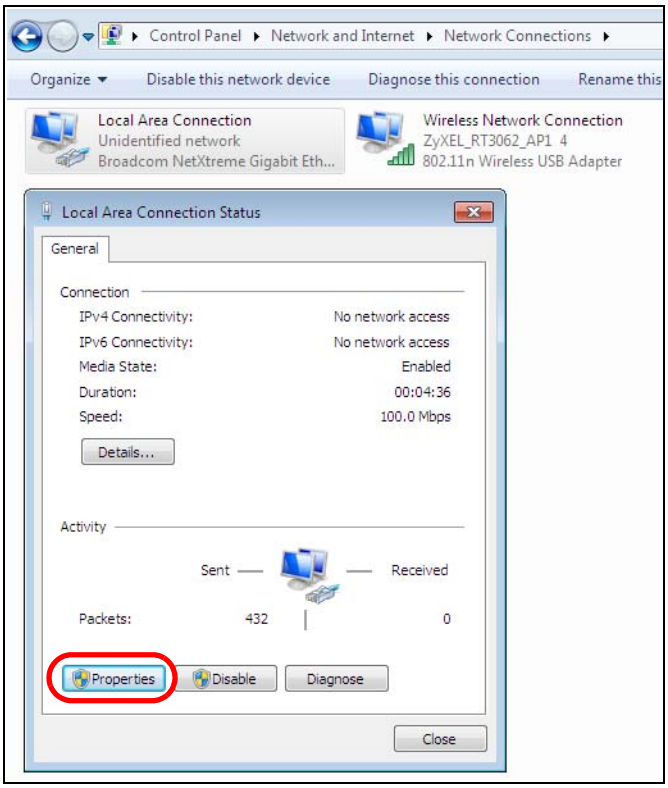
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



3 Click **Change adapter settings**.

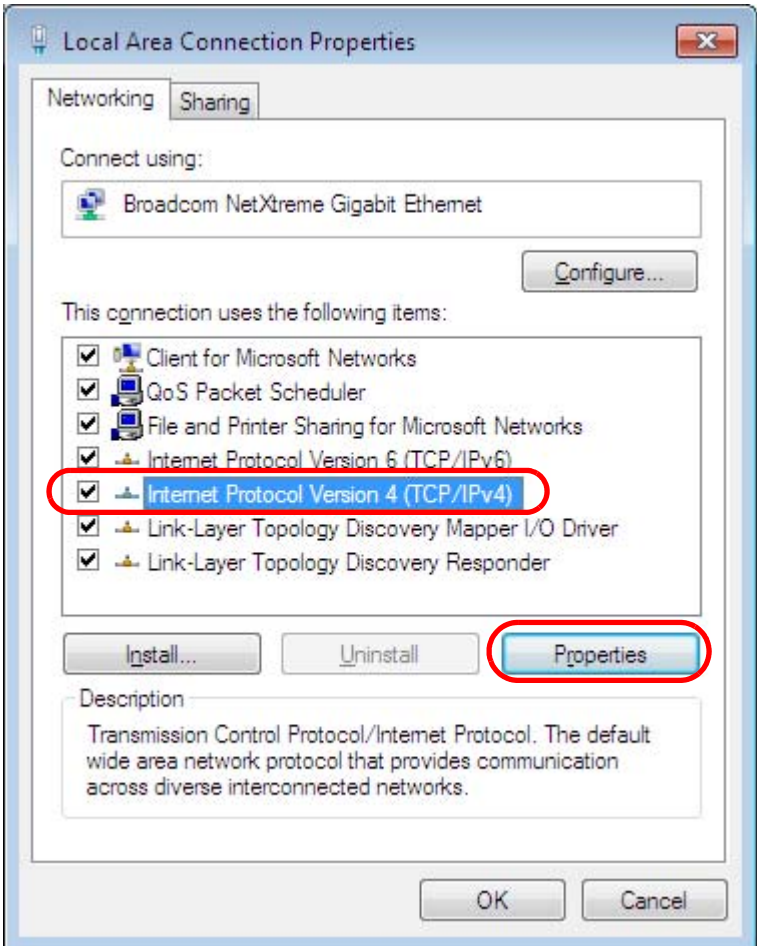


4 Double click **Local Area Connection** and then select **Properties**.

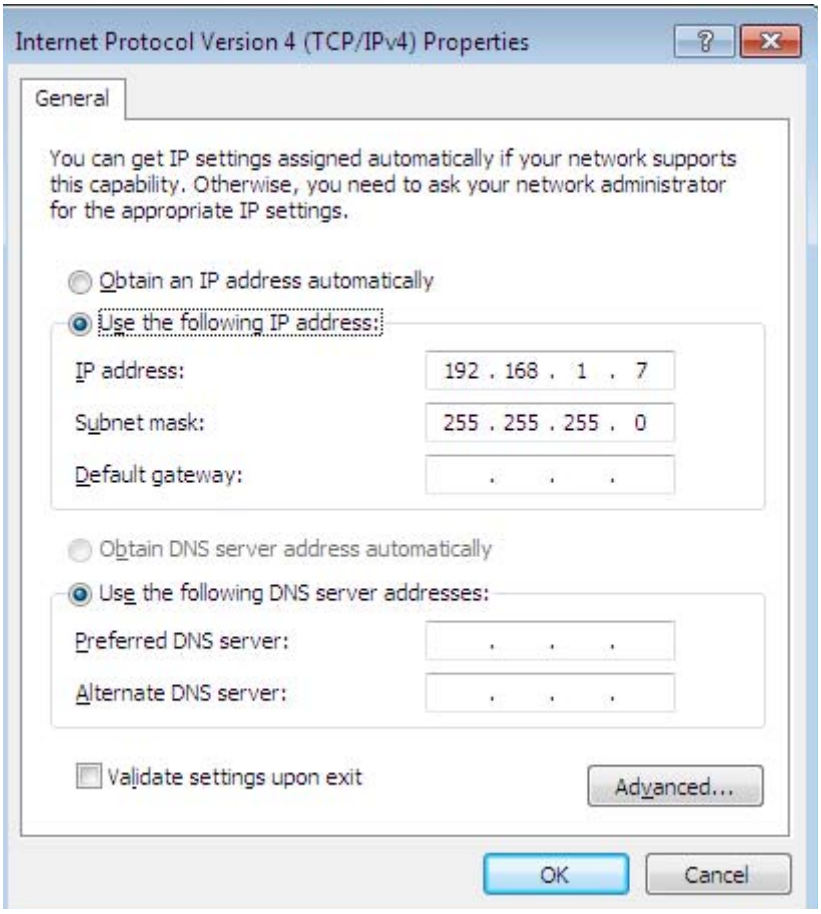


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

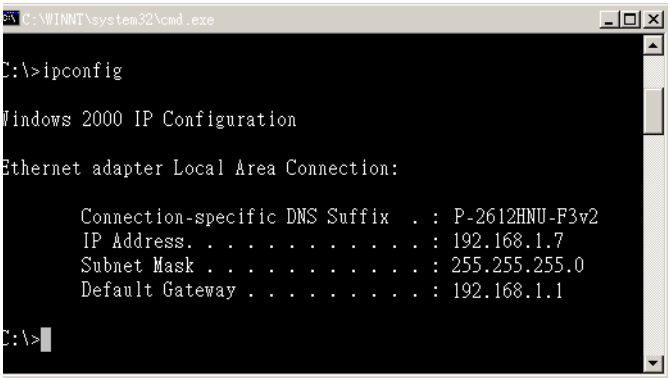
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

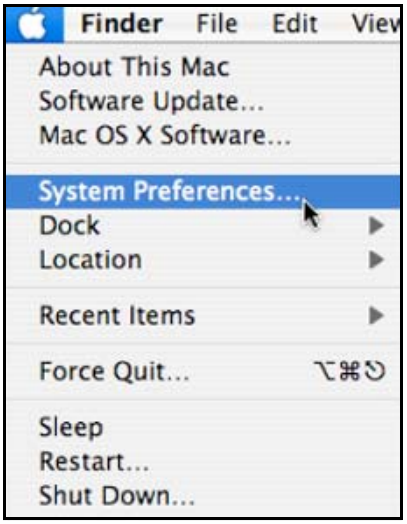
3 The IP settings are displayed as follows.



Mac OS X: 10.3 and 10.4

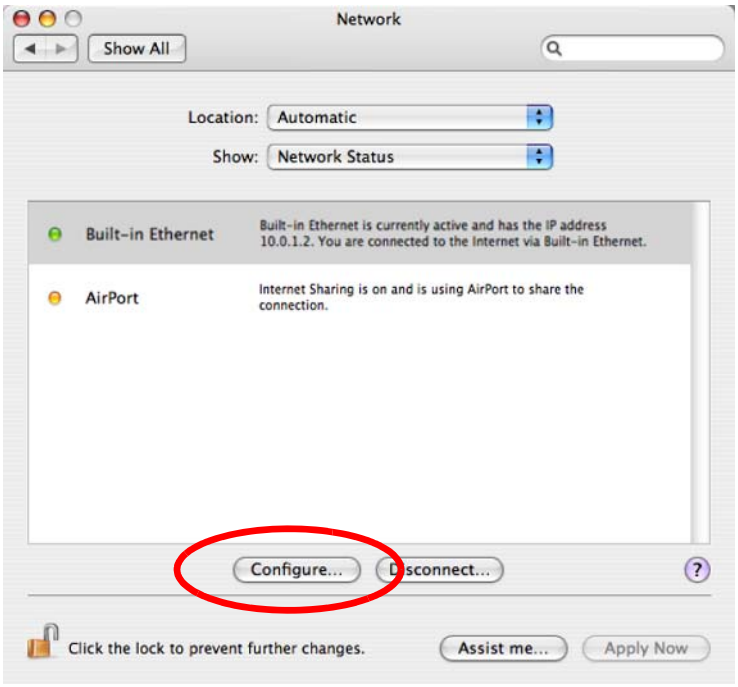
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

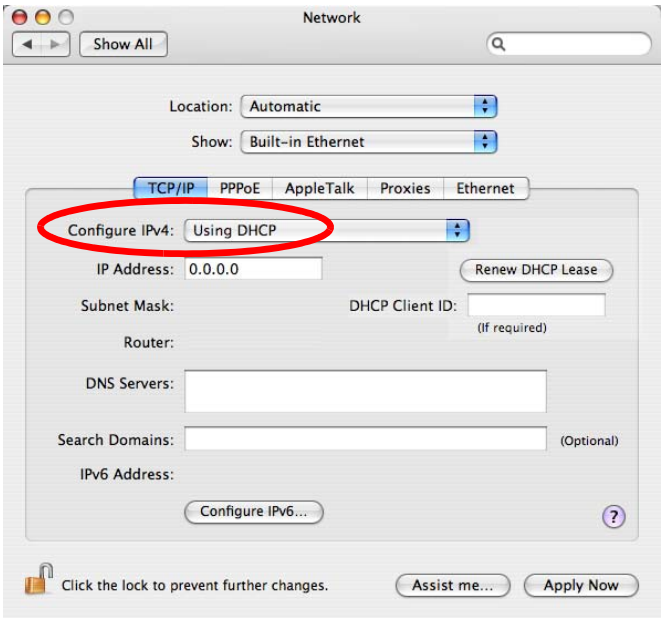


2 In the **System Preferences** window, click the **Network** icon.

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

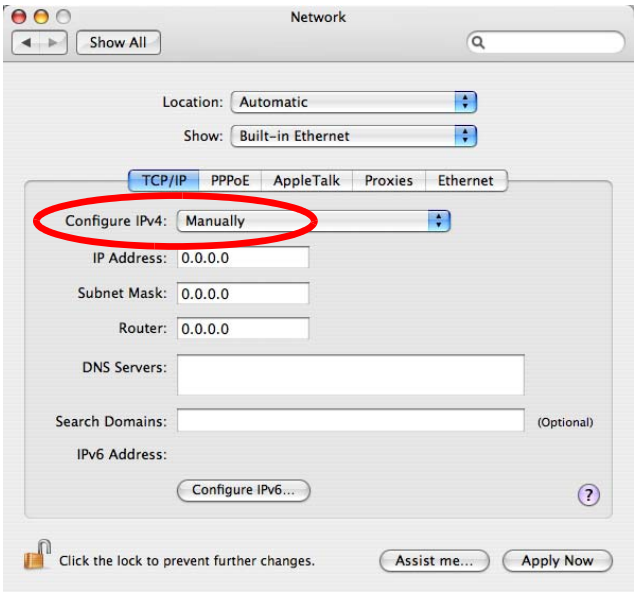


4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

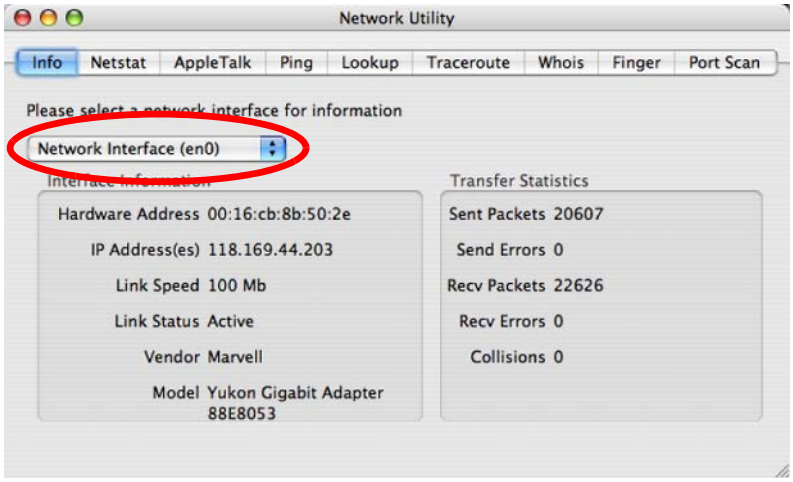


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

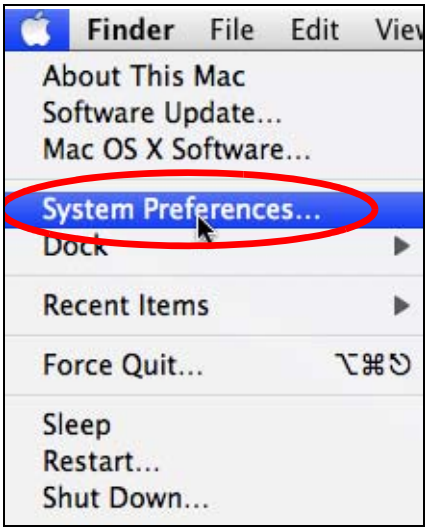
Figure 105 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

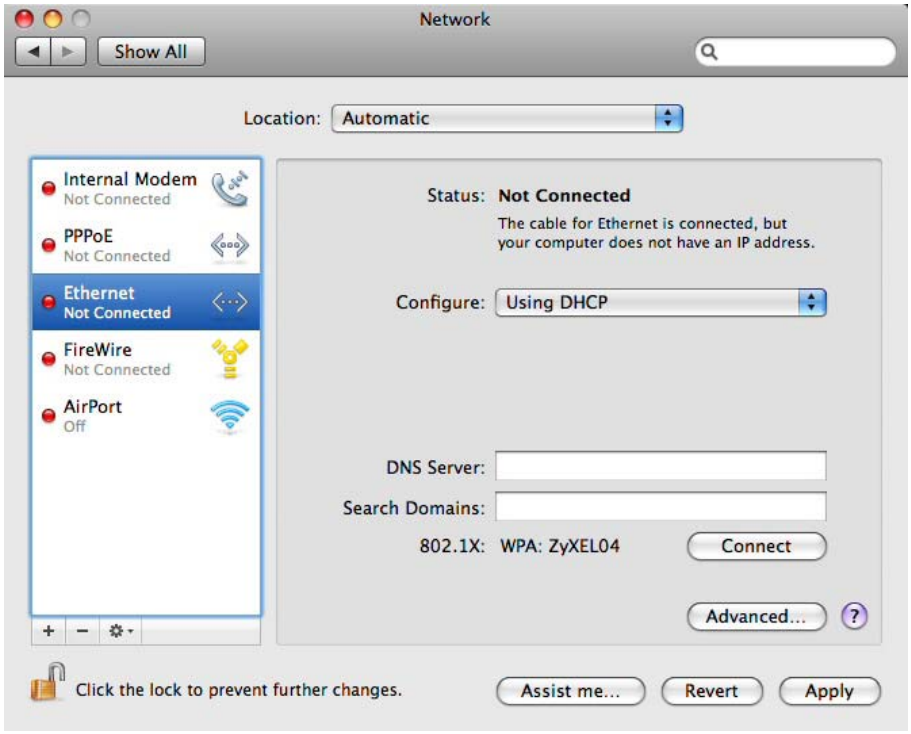
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.



2 In **System Preferences**, click the **Network** icon.

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

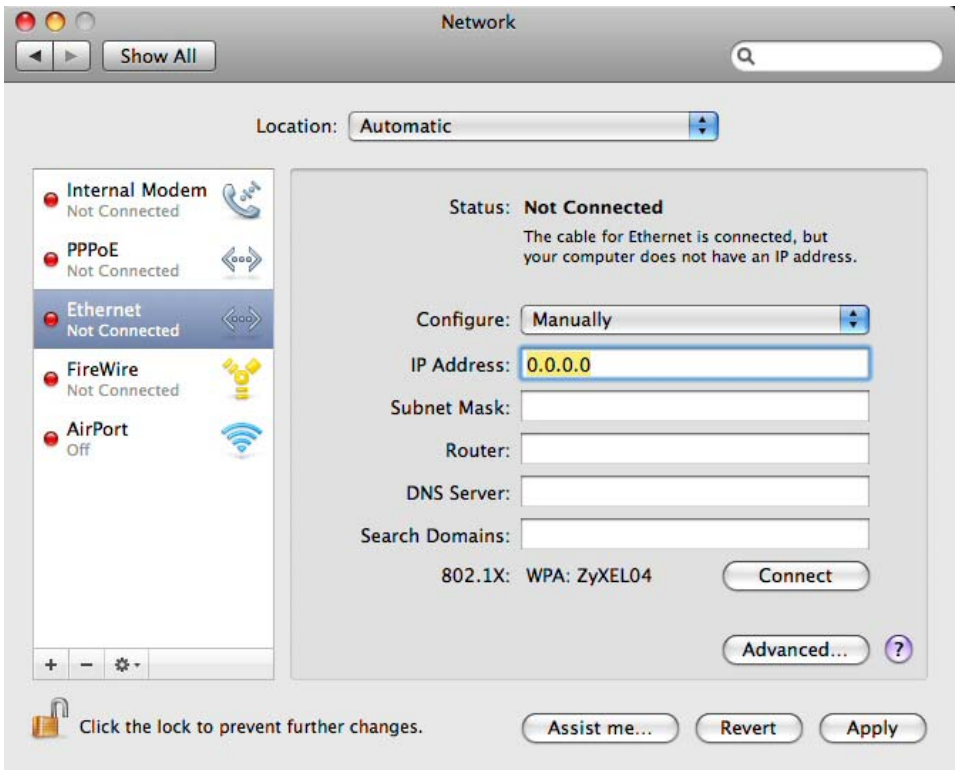


4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.

- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your WAP3205.

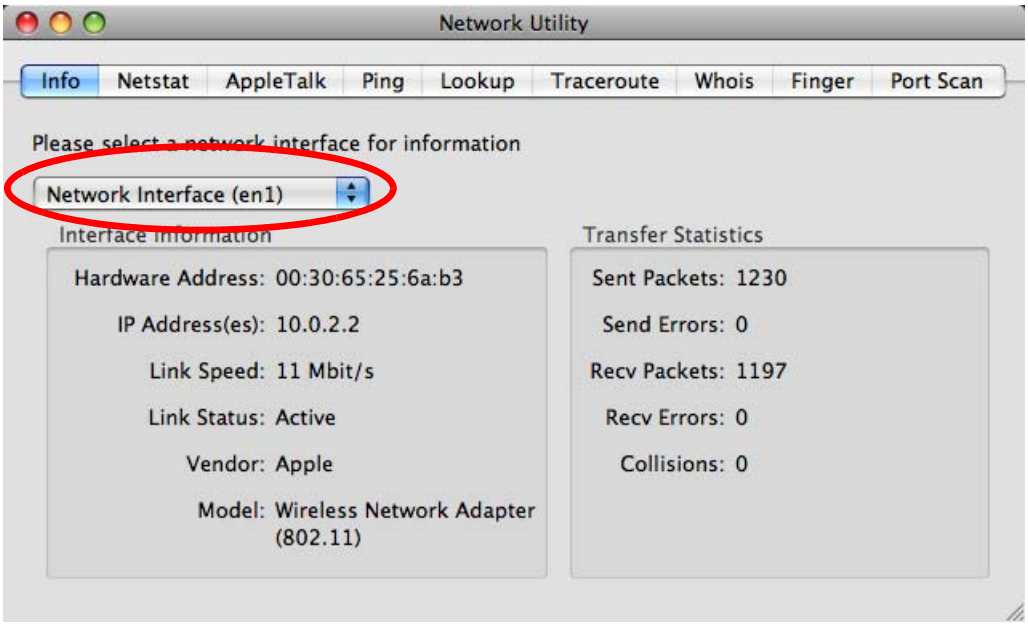


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 106 Mac OS X 10.5: Network Utility



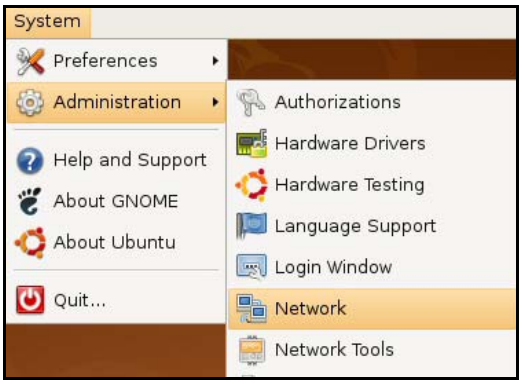
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

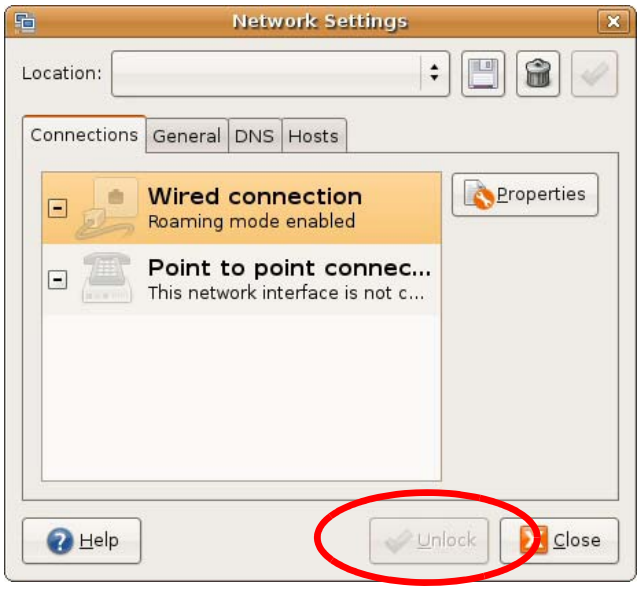
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

1 Click **System > Administration > Network**.



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

5 The **Properties** dialog box opens.

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

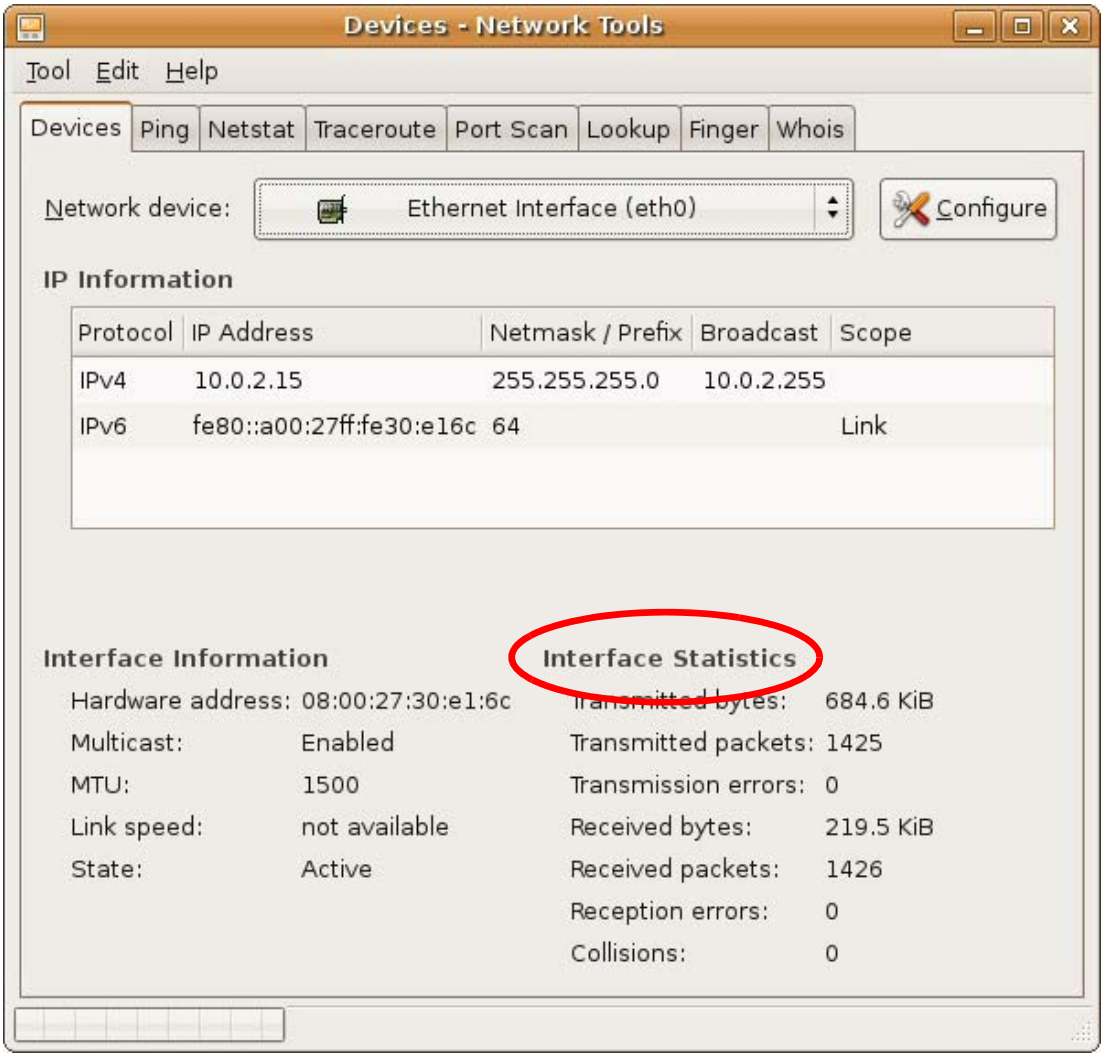
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 107 Ubuntu 8: Network Tools



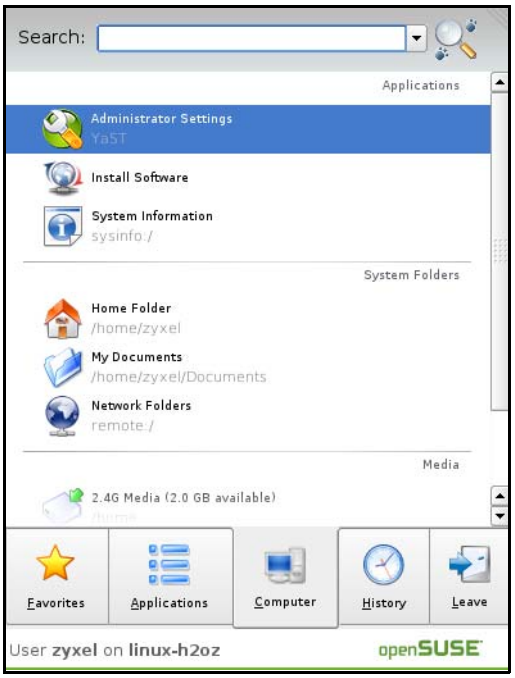
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

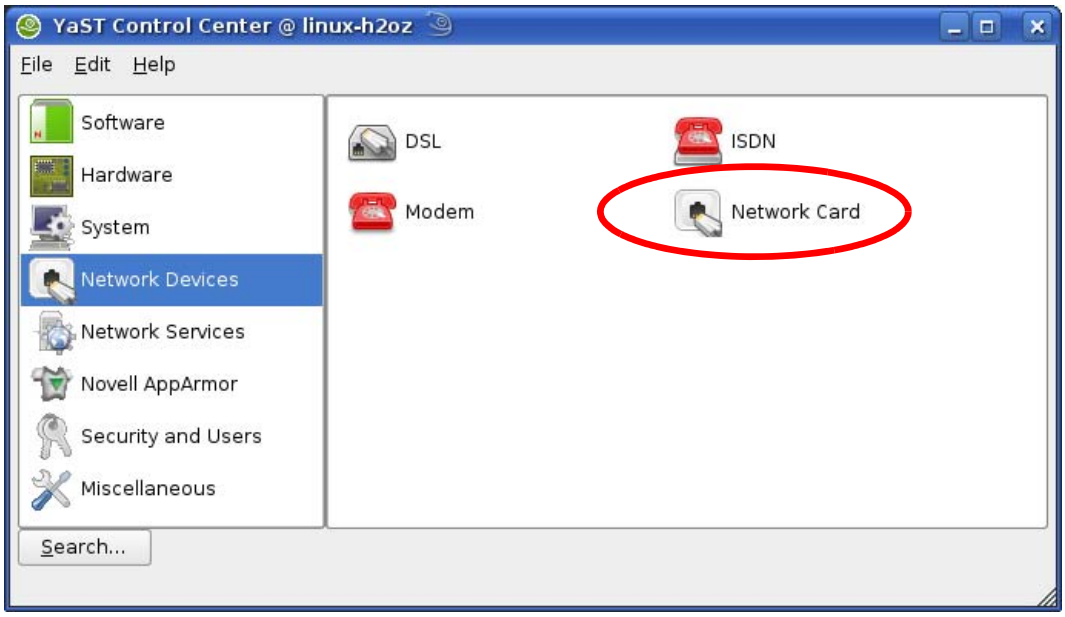
Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

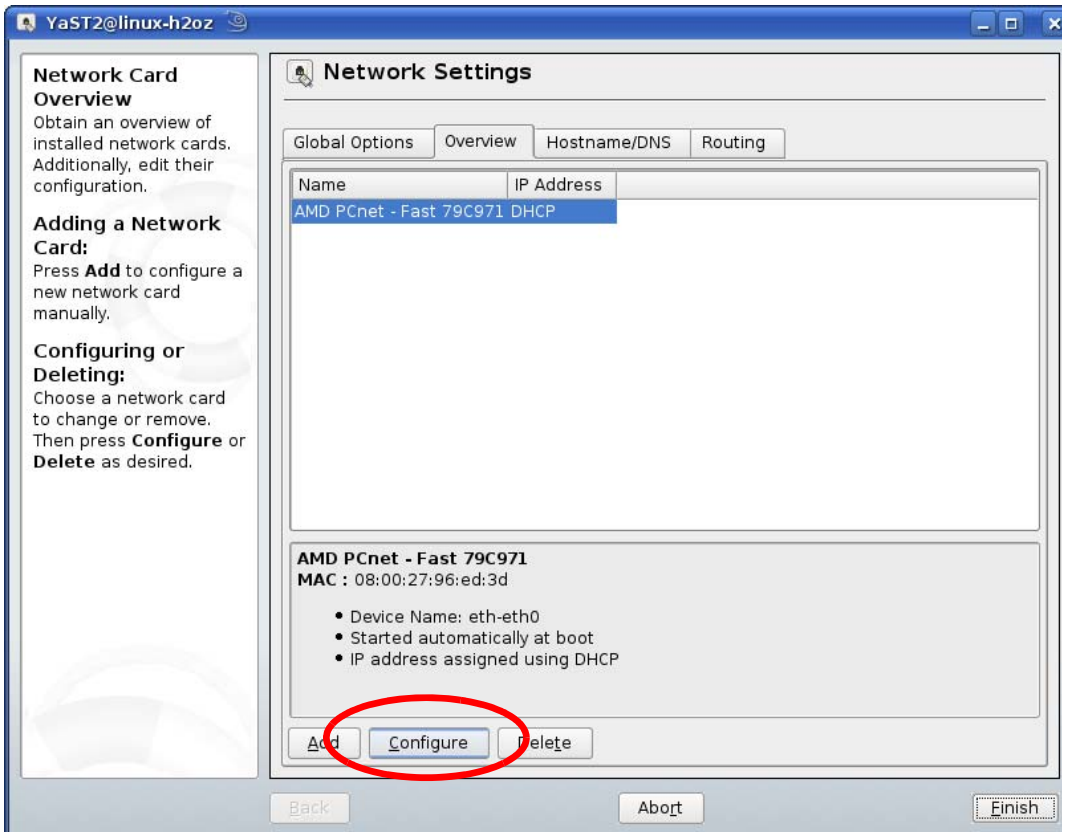


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

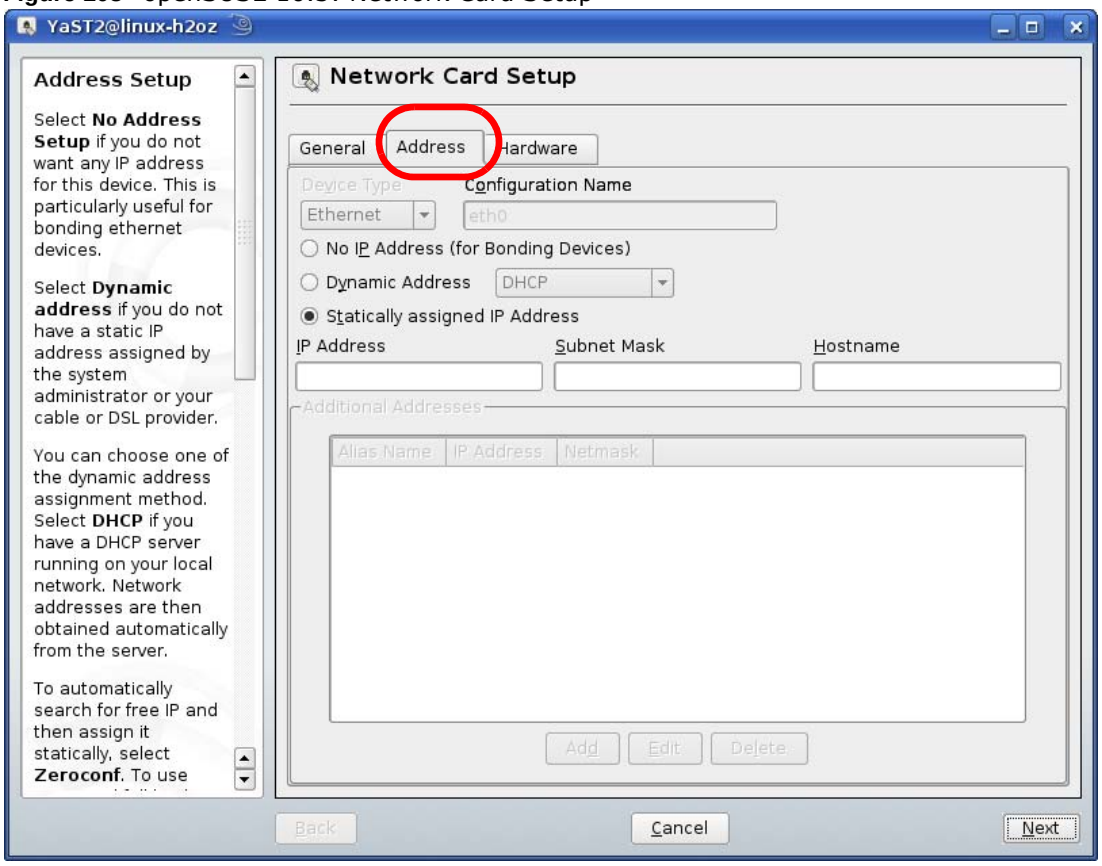


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 108 openSUSE 10.3: Network Card Setup

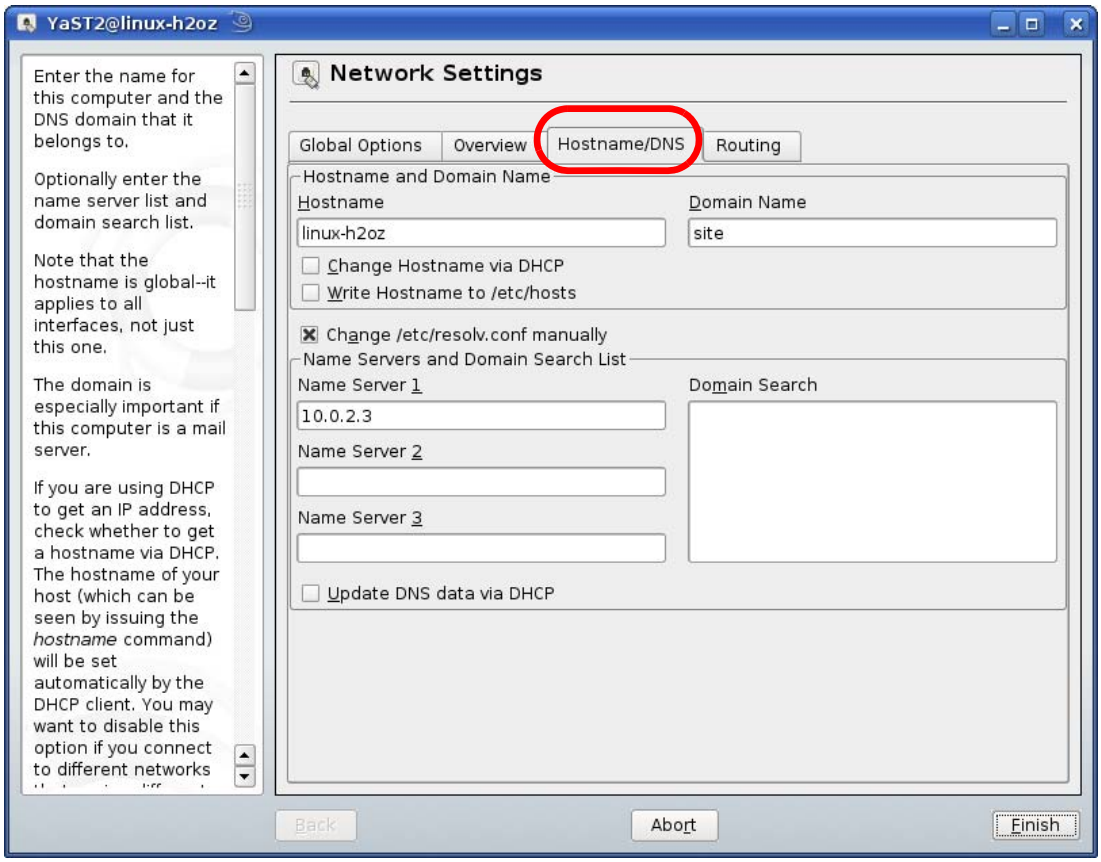


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname / DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.



9 Click **Finish** to save your settings and close the window.

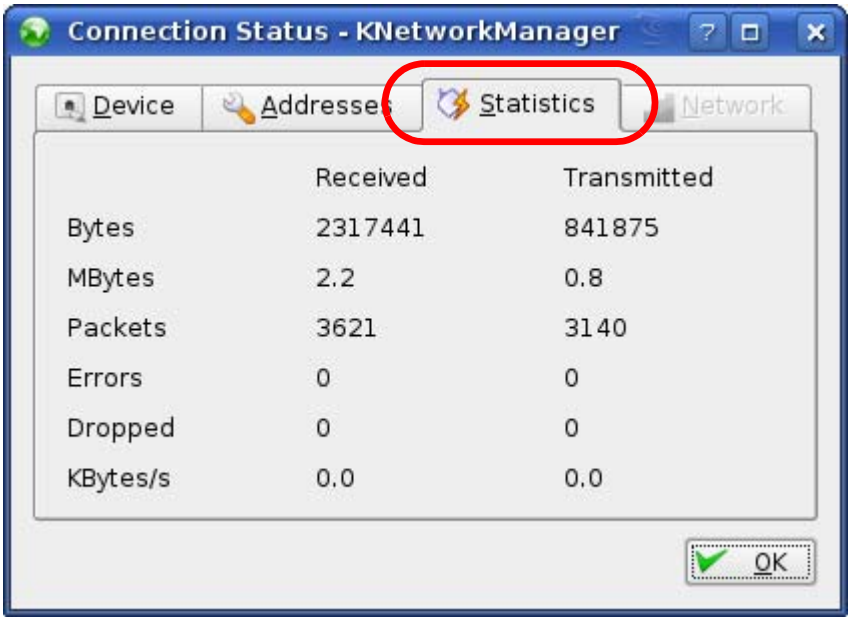
Verifying Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 109 openSUSE 10.3: KNetwork Manager

When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 110 openSUSE: Connection Status - KNetwork Manager



D

Wireless LANs

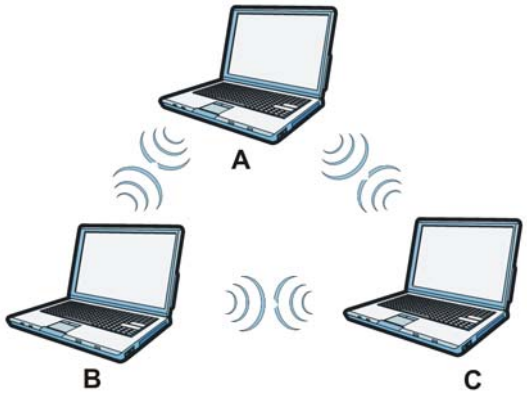
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 111 Peer-to-Peer Communication in an Ad-hoc Network

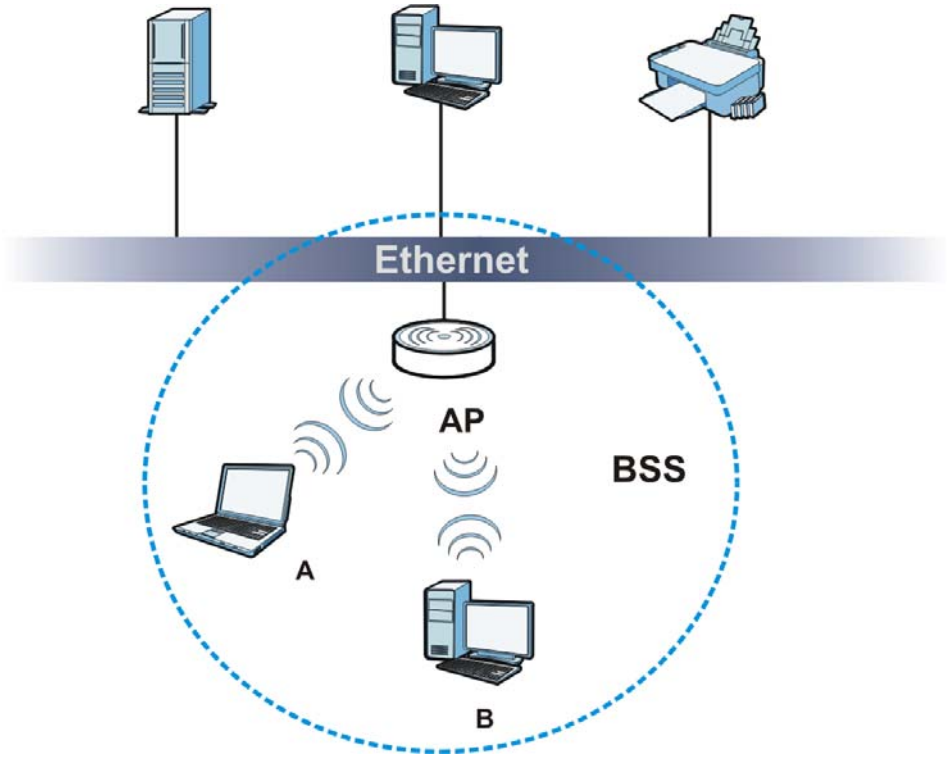


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 112 Basic Service Set



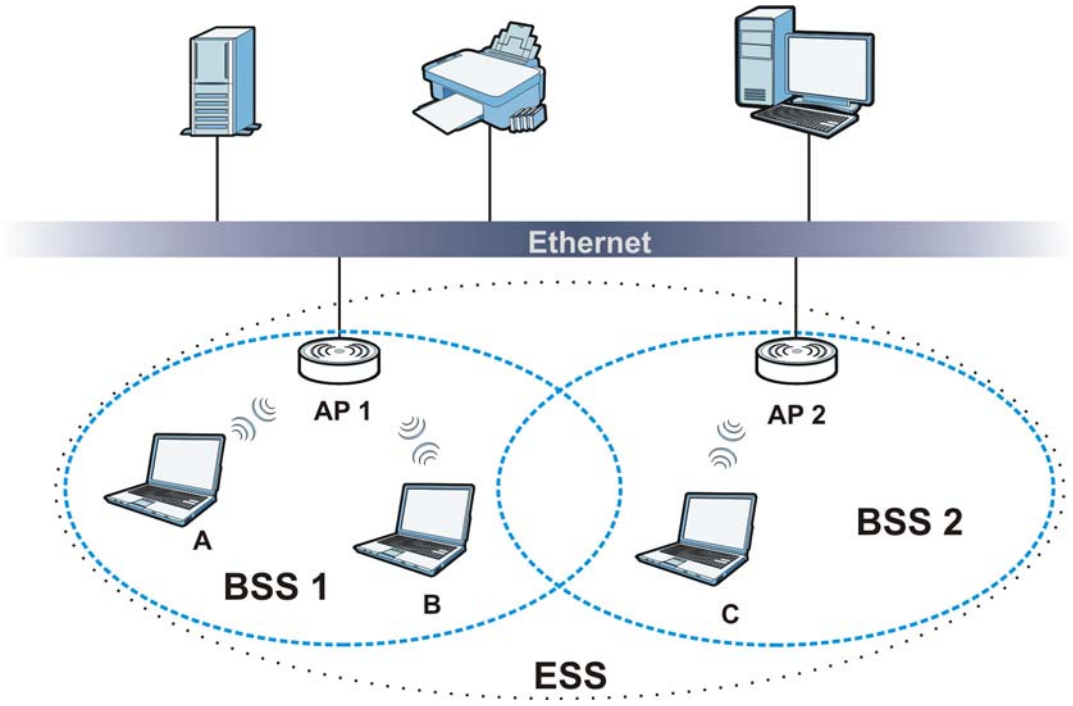
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 113 Infrastructure WLAN



Channel

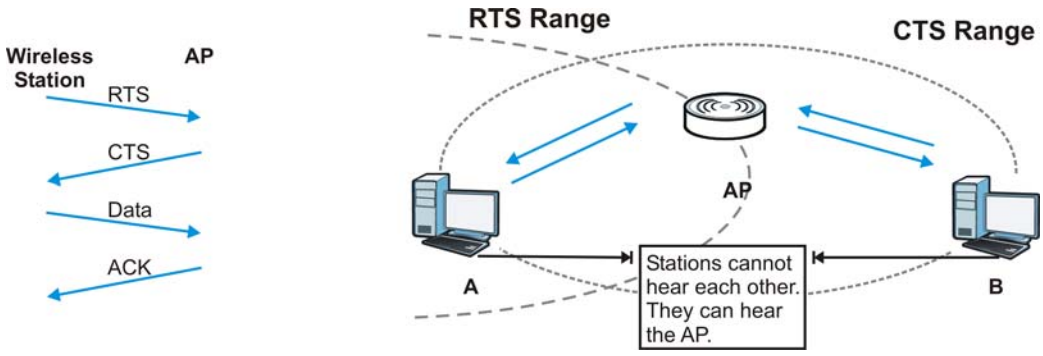
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 114 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the WAP3205 uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 60 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the WAP3205 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the WAP3205 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your WAP3205.

Table 61 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the WAP3205 and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client’s network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 62 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

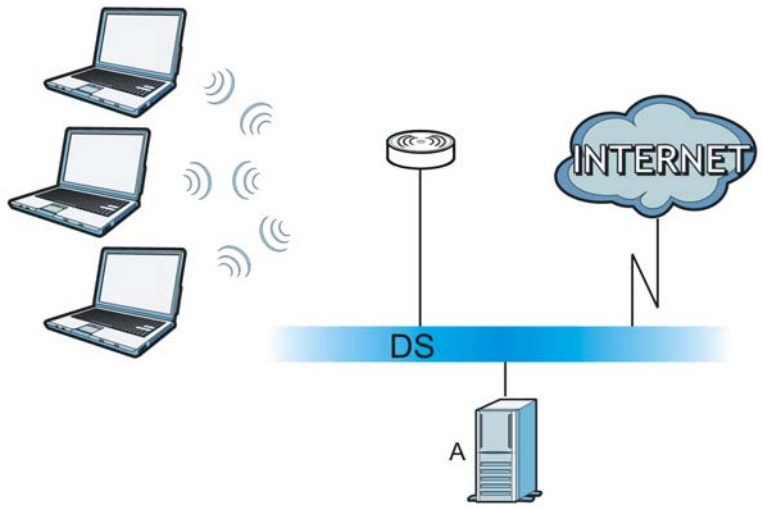
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 115 WPA(2) with RADIUS Application Example



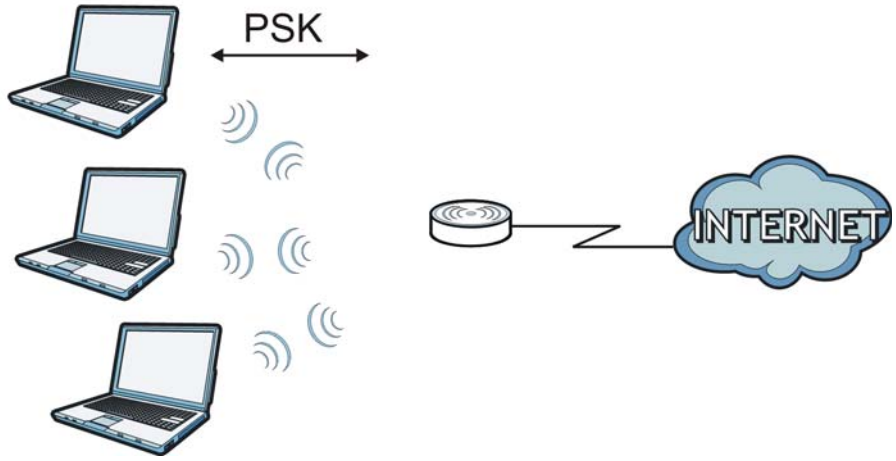
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 116 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 63 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz or 5GHz is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 64 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 64 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

Table 64 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1. this device may not cause interference and
2. this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

CE

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

R&TTE 1999/5/EC		
WLAN 2.4 – 2.4835 GHz		
IEEE 802.11 b/g/n		
Location	Frequency Range(GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).

- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

A

Advanced Encryption Standard
  See AES.
AES 177
alternative subnet mask notation 133
antenna
  directional 181
  gain 181
  omni-directional 181
AP 11
AP (access point) 171
AP Mode
  menu 21
  status screen 18, 24, 36
AP+Bridge 11

B

Basic Service Set, See BSS 169
Bridge/Repeater 11
bridged APs, security 88
BSS 169

C

CA 176
Certificate Authority
  See CA.
certifications 187
  notices 187
  viewing 188
Channel 20, 38
channel 86, 171
  interference 171
Configuration
  restore 111
copyright 187
CPU usage 21, 26, 38
CTS (Clear to Send) 172

D

Daylight saving 108
disclaimer 187
documentation
  related 2
dynamic WEP key exchange 176

E

EAP Authentication 175
encryption 87, 177
  key 87
  WPA compatible 87
ESS 170
Extended Service Set, See ESS 170

F

FCC interference statement 187
Firmware upload 109
  file extension
  using HTTP
firmware version 20, 25, 37
fragmentation threshold 172

G

General wireless LAN screen 88

H

hidden node 171

I

IANA 138
IBSS 169
IEEE 802.11g 173
Independent Basic Service Set
See IBSS 169
initialization vector (IV) 178
Internet Assigned Numbers Authority
See IANA 138
IP Address 104
IP alias 102

L

LAN 101
LAN overview 101
LAN setup 101
LAN TCP/IP 102
Language 111
Link type 20, 26, 38
Local Area Network 101
Log 81

M

MAC 93
MAC address 86
MAC address filter 86
MAC address filtering 93
MAC filter 93
managing the device
good habits 12
using the web configurator. See web configurator.
using the WPS. See WPS.
MBSSID 11
Media access control 93
Memory usage 21, 26, 38
Message Integrity Check (MIC) 177
mode 11

N

NAT 138
Navigation Panel 21
navigation panel 21

O

Operating Channel 20, 38
operating mode 11
other documentation 2

P

Pairwise Master Key (PMK) 178, 179
port speed 20, 26, 38
preamble mode 173
product registration 188
PSK 178

Q

Quality of Service (QoS) 95

R

RADIUS 174
message types 175
messages 175
shared secret key 175
registration
product 188
related documentation 2
Reset button 47

Reset the device 47
Restore configuration 111
Roaming 94
RTS (Request To Send) 172
  threshold 171, 172
RTS/CTS Threshold 86, 94

S

Scheduling 97
Service Set 89
Service Set IDentification 89
Service Set IDentity. See SSID.
SSID 20, 25, 38, 86, 89
subnet 131
Subnet Mask 104
subnet mask 132
subnetting 134
Summary
  Packet statistics 82
  Wireless station status 83
System General Setup 105
System restart 111

T

Temporal Key Integrity Protocol (TKIP) 177
Time setting 107

W

warranty 188
  note 188
Web Configurator
  how to access 43
  Overview 43
web configurator 11
WEP Encryption 29, 31, 39, 40, 41, 91, 92
WEP encryption 90
WEP key 90
Wi-Fi Protected Access 177
Wireless association list 83
wireless client WPA supplicants 178
wireless LAN scheduling 97
Wireless network
  basic guidelines 85
  channel 86
  encryption 87
  example 85
  MAC address filter 86
  overview 85
  security 86
  SSID 86
Wireless security 86
  overview 86
  type 86
wireless security 173
Wireless tutorial 59
  WPS 59
Wizard setup 49
WLAN
  interference 171
  security parameters 180
WPA 177
  key caching 178
  pre-authentication 178
  user authentication 178
  vs WPA-PSK 178
  wireless client supplicant 178
  with RADIUS application example 179
WPA compatible 87
WPA2 177
  user authentication 178
  vs WPA2-PSK 178
  wireless client supplicant 178
  with RADIUS application example 179
WPA2-Pre-Shared Key 177
WPA2-PSK 177, 178
  application example 179
WPA-PSK 177, 178
  application example 179
WPS 11